Государственное образовательное учреждение
высшего профессионального образования
**«Томский государственный университет
систем управления и радиоэлектроники»**

ТЕМАТИЧЕСКИЙ РЕФЕРАТИВНЫЙ СБОРНИК № 7-1

“Information Protection”
(«Защита информации»)

Журнальные публикации

Источник: *Digital Library IEEEXplore*
Язык: *английский*
Глубина поиска: *2006 – 2011 гг.*
Дата формирования: *март 2011 г.*
Составитель: *В.И. Карнышев*

Томск – 2011

ТЕМАТИЧЕСКИЙ РЕФЕРАТИВНЫЙ СБОРНИК № 7-1

"Information Protection"
(«Защита информации»)
Журнальные публикации

"Unequal Error Protection Using Fountain Codes With Applications to Video Communication"

Application-layer forward error correction (FEC) is used in many multimedia communication systems to address the problem of packet loss in lossy packet networks. One powerful form of application-layer FEC is unequal error protection which protects the information symbols according to their importance. We propose a method for unequal error protection with a Fountain code. When the information symbols were partitioned into two protection classes (most important and least important), our method required a smaller transmission bit budget to achieve low bit error rates compared to the two state-of-the-art techniques. We also compared our method to the two state-of-the-art techniques for video unicast and multicast over a lossy network. Simulations for the scalable video coding (SVC) extension of the H.264/AVC standard showed that our method required a smaller transmission bit budget to achieve high-quality video. [J1]

"Exploiting Trust-Based Social Networks for Distributed Protection of Sensitive Data"

How can we protect sensitive data of average users? In this paper, we propose taking advantage of real-life social trust between average users (called "trust-based social networks") as well as threshold cryptography. This leads to a new type of complex systems, for which we define and characterize the following novel properties: 1) attack-resilience, which captures the consequences of computers getting compromised; 2) security utility of anonymous social networks, which captures the security gained when the underlying social network links are not known to the attacker; 3) security utility of psychological soundness, which captures the security gained when a user keeps a decisive share of its sensitive data; 4) availability, which captures the effect when computers are not always responsive; 5) the trade-off between attack-resilience and availability. [J2]

"An Integrated Framework for Smart Microgrids Modeling, Monitoring, Control, Communication, and Verification"

The microgrid (MG) paradigm is a new concept which is considered as a solution for addressing technical, economical, and environmental issues of modern power systems. The application of MG is the subject of extensive studies and experimental tests. It is recognized that there are a number of technical challenges concerning the operation, monitoring, control, and protection of MGs systems. In this respect, the rapid development of the information and communication technologies (ICTs) has opened the door for feasible and cost-effective solutions allowing more extensive intra- and interutility information exchange, diffusion, and open access to a wide range of real-time information. Consequently, the ICTs could represent a strategic tool in supporting effective MG operation. According to this statement, the paper proposes an advanced framework based on the service-oriented architectures for integrated MG modeling, monitoring, and control. The proposed framework is platform, language, and vendor independent, and thus it is an ideal candidate for an effective integration in existing energy management systems and distribution management systems (EMSs/DMSs). [J3]

"Privacy Protection of Fingerprint Database"

A fingerprint authentication system for the privacy protection of the fingerprint template stored in a database is introduced here. The considered fingerprint data is a binary thinned fingerprint image, which will be embedded with some private user information without causing obvious abnormality in the enrollment phase. In the authentication phase, these hidden user data can be extracted from the stored template for verifying the authenticity of the person who provides the query fingerprint. A novel data hiding scheme is proposed for the thinned fingerprint template. This scheme does not produce any boundary pixel in the thinned fingerprint during data embedding. Thus, the abnormality caused by data hiding is visually imperceptible in the marked-thinned fingerprint. Compared with using existing binary image data hiding techniques, the proposed method causes the least abnormality for a thinned fingerprint without compromising the performance of the fingerprint identification. [J4]

"A Privacy-Preserving Buyer-Seller Watermarking Protocol Based on Priced Oblivious Transfer"

Buyer-seller watermarking protocols allow copyright protection of digital goods. To protect privacy, some of those protocols provide buyers with anonymity. However, anonymous e-commerce protocols pose several disadvantages, like hindering customer management or requiring anonymous payment mechanisms. Additionally, no existing buyer-seller watermarking protocol provides fair exchange. We propose a novel approach for the design of privacy-preserving buyer-seller watermarking protocols. In our approach, the seller authenticates buyers but does not learn which items are purchased. Since buyers are not anonymous, customer management is eased and currently deployed methods of payment can be utilized. We define an ideal functionality for privacy-preserving copyright protection protocols. To realize our functionality, a protocol must ensure that buyers pay the right price without disclosing the purchased item, and that sellers are able to identify buyers that released pirated copies. We construct a protocol based on priced oblivious transfer and on existing techniques for asymmetric watermark embedding. Furthermore, we implement and evaluate the efficiency of our protocol, and we explain how to extend it in order to achieve optimistic fair exchange. [J5]

"An Obfuscation-Based Approach for Protecting Location Privacy"

The pervasive diffusion of mobile communication devices and the technical improvements of location techniques are fostering the development of new applications that use the physical position of users to offer location-based services for business, social, or informational purposes. In such a context, privacy concerns are increasing and call for sophisticated solutions able to guarantee different levels of location privacy to the users. In this paper, we address this problem and present a solution based on different obfuscation operators that, when used individually or in combination, protect the privacy of the location information of users. We also introduce an adversary model and provide an analysis of the proposed obfuscation operators to evaluate their robustness against adversaries aiming to reverse the obfuscation effects to retrieve a location that better approximates the location of the users. Finally, we present some experimental results that validate our solution. [J6]

"Preventing the Decodability Attack Based Cross-Matching in a Fuzzy Commitment Scheme"

Template protection techniques are used within biometric systems in order to safeguard the privacy of the system's subjects. This protection also includes unlinkability, i.e., preventing cross-matching between two or more reference templates from the same subject across different applications. In the literature, the template protection techniques based on fuzzy commitment, also known as the code-offset construction, have recently been investigated. Recent work presented the decodability attack vulnerability facilitating cross-matching based on the protected templates and its theoretical analysis. First, we extend the theoretical analysis and include the comparison between the system and cross-matching performance. We validate the presented analysis using real biometric data from the MCYT fingerprint database. Second, we show that applying a random bit-permutation process secures the fuzzy commitment scheme from cross-matching based on the decodability attack. [J7]

"Privacy-Preserving OLAP: An Information-Theoretic Approach"

We address issues related to the protection of private information in Online Analytical Processing (OLAP) systems, where a major privacy concern is the adversarial inference of private information from OLAP query answers. Most previous work on privacy-preserving OLAP focuses on a single aggregate function and/or addresses only exact disclosure, which eliminates from consideration an important class of privacy breaches where partial information, but not exact values, of private data is disclosed (i.e., partial disclosure). We address privacy protection against both exact and partial disclosure in OLAP systems with mixed aggregate functions. In particular, we propose an information-theoretic inference control approach that supports a combination of common aggregate functions (e.g., COUNT, SUM, MIN, MAX, and MEDIAN) and guarantees the level of privacy disclosure not to exceed thresholds predetermined by the data owners. We demonstrate that our approach is efficient and can be implemented in existing OLAP systems with little modification. It also satisfies the simulatable auditing model and leaks no private information through query rejections. Through performance analysis, we show that compared with previous approaches, our approach provides more effective privacy protection while maintaining a higher level of query-answer availability. [J8]

"Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks"

Wide-area monitoring, protection, and control (WAMPAC) involves the use of system-wide information and the communication of selected local information to a remote location to counteract the propagation of large disturbances. Synchronized measurement technology (SMT) is an important element and enabler of WAMPAC. It is expected that WAMPAC systems will in the future reduce the number of catastrophic blackouts and generally improve the reliability and security of energy production, transmission, and distribution, particularly in power networks with a high level of operational uncertainties. In this paper, the technological and application issues are

addressed. Several key monitoring, protection, and control applications are described and discussed. A strategy for developing a WAMPAC system in the United Kingdom is given as well. [J9]

"OFDM-Based Common Control Channel Design for Cognitive Radio Ad Hoc Networks"

Cognitive radio (CR) technology allows devices to opportunistically use the vacant portions of the licensed wireless spectrum. However, the available spectrum changes dynamically with the primary user (PU) activity, necessitating frequent PU sensing coordination and exchanging network topology information in a multihop CR ad hoc network. To facilitate these tasks, an always-on, out-of-band common control channel (CCC) design is proposed that uses noncontiguous OFDM subcarriers placed within the guard bands separating the channels of the licensed spectrum. First, the task of choosing the OFDM-specific parameters, including the number, power, and bandwidth of the subcarriers is formulated as a feasibility problem to ensure that the CCC does not adversely interfere with the PU operation. Second, for unicast messaging between a given pair of users, a subset of the guard bands may be chosen, which allows an additional measure of protection for the adjacent PU spectrum. For this, the multiarm bandit algorithm is used that allows the guard band selection to evolve over time based on the observed interference from the PU. Results reveal that our proposed CCC ensures connectivity and improved PU protection with a limited trade-off in data rate when compared to frequency-hopping and cluster-based CCC schemes. [J10]

"Papel: Provenance-Aware Policy Definition and Execution"

Data processing is often restricted by contractual and legal requirements for protecting privacy and intellectual-property rights. Internet policies help control how and by whom data is processed. Policy conditions could depend on previous data processing and thus on the processing histories' temporal structure. However, existing policy languages don't allow for expressing the temporal aspects of such conditions. Papel (Provenance-Aware Policy Definition and Execution Language) uses provenance information to connect data-processing policies and histories and to map the processing histories' temporal structure to a graph structure. [J11]

"Iterative Encoder-Controller Design for Feedback Control Over Noisy Channels"

We study a closed-loop control system with state feedback transmitted over a noisy discrete memoryless channel. With the objective to minimize the expected linear quadratic cost over a finite horizon, we propose a joint design of the sensor measurement quantization, channel error protection, and controller actuation. It is argued that despite that this encoder-controller optimization problem is known to be hard in general, an iterative design procedure can be derived in which the controller is optimized for a fixed encoder, then the encoder is optimized for a fixed controller, etc. Several properties of such a scheme are discussed. For a fixed encoder, we study how to optimize the controller given that full or partial side-information is available at the encoder about the symbols received at the controller. It is shown that the certainty equivalence controller is optimal when the encoder is optimal and has full side-information. For a fixed controller, expressions for the optimal encoder are given and implications are discussed for the special cases when process, sensor, or channel noise is not present. Numerical experiments are carried out to demonstrate the performance obtained by employing the proposed iterative design procedure and to compare it with other relevant schemes. [J12]

"Analysis of Underfrequency Load Shedding Using a Frequency Gradient"

Underfrequency load shedding is one of the most important protection systems, as in many cases it represents the last chance to prevent a system blackout after a serious disturbance occurs in a power system. In order to improve traditional schemes, many efforts have been concentrated on attempts to use the frequency gradient as an indicator for determining the lack of active power in a system. This paper concentrates on analyzing the factors that influence the gradient. Analyses have shown that the gradient can give misleading information about the active-power deficit, as long as certain factors are ignored or assumed to be constant. A draft of a gradient-based underfrequency load-shedding scheme is presented, which also highlights the problems associated with the use of gradient. On the one hand, a frequency gradient alone does not appear to be sufficient for the active-power deficit estimation. Nevertheless, for the actual load-shedding procedure it is found to be very useful. [J13]

"Urban Infrastructure-to-Vehicle Traffic Data Dissemination Using UEP Rateless Codes"

In this paper we propose an end-to-end solution for urban infrastructure-to-vehicle traffic data delivery based on a class of unequal error protection (UEP) rateless codes called expanding window fountain (EWF) codes. The proposed solution relies on attractive features that rateless codes introduce to networks with unpredictable dynamics: the universal capacity approaching property which is well-matched to time-varying behavior of wireless links, and the innovative nature of each encoded packet which makes both time-consuming retransmission and content-reconciliation mechanisms unnecessary. Furthermore, usage of EWF codes allows separation of

delivered data in importance classes with different error protection and recovery time guarantees, enabling mobile users to retrieve more important information more reliably and in shorter time span, thus making the proposed solution suitable for time-critical services. The addressed urban communication scenario consists of large number of sensors that sample and relay traffic flow information to network of Access Points (APs). APs use the existing underlying communication infrastructure, such as metropolitan area networks (MANs), to exchange traffic flow data, encode it using EWF coding principles, and finally disseminate it to roaming vehicles that join the network service in an ad-hoc manner in order to retrieve information regarding the surrounding environment. The proposed approach is suitable for real-time applications, such as frequent periodic reporting of urban traffic conditions, that could be used by on-board computers to provide improved navigation for end-users. [J14]

"A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting"

A video copy detection system that is based on content fingerprinting and can be used for video indexing and copyright applications is proposed. The system relies on a fingerprint extraction algorithm followed by a fast approximate search algorithm. The fingerprint extraction algorithm extracts compact content-based signatures from special images constructed from the video. Each such image represents a short segment of the video and contains temporal as well as spatial information about the video segment. These images are denoted by temporally informative representative images. To find whether a query video (or a part of it) is copied from a video in a video database, the fingerprints of all the videos in the database are extracted and stored in advance. The search algorithm searches the stored fingerprints to find close enough matches for the fingerprints of the query video. The proposed fast approximate search algorithm facilitates the online application of the system to a large video database of tens of millions of fingerprints, so that a match (if it exists) is found in a few seconds. The proposed system is tested on a database of 200 videos in the presence of different types of distortions such as noise, changes in brightness/contrast, frame loss, shift, rotation, and time shift. It yields a high average true positive rate of 97.6% and a low average false positive rate of 1.0%. These results emphasize the robustness and discrimination properties of the proposed copy detection system. As security of a fingerprinting system is important for certain applications such as copyright protections, a secure version of the system is also presented. [J15]

"Database Access Pattern Protection Without Full-Shuffles"

Privacy protection is one of the fundamental security requirements for database outsourcing. A major threat is information leakage from database access patterns generated by query executions. The standard private information retrieval (PIR) schemes, which are widely regarded as theoretical solutions, entail O(n) computational overhead per query for a database with nitems. Recent works propose to protect access patterns by introducing a trusted component with constant storage size. The resulting privacy assurance is as strong as PIR, though with O(1) online computation cost, they still have O(n) amortized cost per query due to periodically full database shuffles. In this paper, we design a novel scheme in the same model with provable security, which only shuffles a portion of the database. The amortized server computational complexity is reduced to O(√{nlogn/k}). With a secure storage storing thousands of items, our scheme can protect the access pattern privacy of databases of billions of entries, at a lower cost than those using ORAM-based poly-logarithm algorithms. [J16]

"Service Usage Accounting"

When a party provides service and wishes to receive compensation for the provision of its resources, the question of getting assured accounting information also emerges. Although various prepaid or postpaid solutions can be devised, it does not provide very good protection if the service is not received after the payment or the user disputes the bill. We present, in this article, a network-level, service-usage solution, which provides assured accounting information strongly bound to the host identity, so that the user is unable to repudiate the charges. To protect the user, the solution employs a granular approach, where evidence of service usage is provided in a piecemeal manner, i.e., pay as you go. An implementation of such a solution is presented, which is based on the employment of host identity protocol (HIP) and hash chains. [J17]

"CRP: A Routing Protocol for Cognitive Radio Ad Hoc Networks"

Cognitive radio (CR) technology enables the opportunistic use of the vacant licensed frequency bands, thereby improving the spectrum utilization. However, the CR operation must not interfere with the transmissions of the licensed or primary users (PUs), and this is generally achieved by incurring a trade-off in the CR network performance. In order to evaluate this trade-off, a distributed CR routing protocol for ad hoc networks (CRP) is proposed that makes the following contributions: (i) explicit protection for PU receivers that are generally not detected during spectrum sensing, (ii) allowing multiple classes of routes based on service differentiation in CR

networks, and (iii) scalable, joint route-spectrum selection. A key novelty of CRP is the mapping of spectrum selection metrics, and local PU interference observations to a packet forwarding delay over the control channel. This allows the route formation undertaken over a control channel to capture the environmental and spectrum information for all the intermediate nodes, thereby reducing the computational overhead at the destination. Results reveal the importance of formulating the routing problem from the viewpoint of safeguarding the PU communication, which is a unique feature in CR networks. [J18]

"Zero-Knowledge Sets With Short Proofs"

Zero knowledge sets (ZKS), introduced by Micali, Rabin, and Kilian in 2003, allow a prover to commit to a secret set Sin a way such that it can later prove, non interactively, statements of the form $xin S$(or $xnotin S$), without revealing any further information (on top of what explicitly revealed by the inclusion/exclusion statements above) on S, not even its size. Later, Chase Field=03 ed away the Micali, Rabin, and Kilian's construction by introducing an elegant new variant of commitments that they called (trapdoor) mercurial commitments. Using this primitive, it was shown how to construct zero knowledge sets from a variety of assumptions (both general and number theoretic). This paper introduces the notion of trapdoor q-mercurial commitments (${ssr qTMC}$s), a notion of mercurial commitment that allows the sender to commit to an ordered sequence of exactly $q$messages, rather than to a single one. Following the previous work, it is shown how to construct ZKS from ${ssr qTMC}$s and collision resistant hash functions. Then, it is presented an efficient realization of ${ssr qTMC}$s that is secure under the so called Strong Diffie Hellman (SDH) assumption, a number theoretic conjecture recently introduced by Boneh and Boyen. Using such scheme as basic building block, it is obtained a construction of ZKS that allows for proofs that are much shorter with respe--ct to the best previously known implementations. In particular, for an appropriate choice of the parameters, our proofs are up to 33% shorter for the case of proofs of membership, and up to 73% shorter for the case of proofs of nonmembership. Experimental tests confirm practical time performances. [J19]

"Sender Scorecards"

Unsolicited communication is a major issue in digital communications and for the networks enabling such communication. With the increasing use of IP multimedia subsystem (IMS) networks, protection of time-critical communication, e.g., voice over IP (VoIP), from unsolicited messages becomes an important topic. The protection against unsolicited communication for IMS (PUCI) borrows the concepts from traditional e-mail spam filtering but needs to adapt to the nature of IMS communication being direct and time critical. In addition to the protection methods identified in TR 33.937 [1], we present a concept that uses a secure and interoperable scorecard that is associated with the caller and IMS communication. Depending on the outcome of the scorecard evaluation, the receiving domain can take appropriate actions such as denying or allowing a communication attempt. Scorecards are used to generate a standardized exchange format for the sender- and message-related information. Based on Third Generation Partnership Project (3GPP) standards, we present an IMS architecture with scorecard elements, including basic operating procedures for the prevention of unsolicited communication for IMS (UCI). [J20]

"Field Analysis of the Occurrence of Distribution-Line Faults Caused by Lightning Effects"

Electric supply reliability is an issue of wide importance to both an information-oriented society and electric power companies. This paper focuses on lightning effects on distribution lines. Field research is now underway in the northern part of the Kanto Plain in Japan, and voltage and current waveforms in distribution lines due to lightning hits have been observed since 1996. There are now 284 datasets; these include data on 62 direct flashes to lines. This research reveals that a distribution line can be protected from direct lightning strokes. In some cases, no power follow current was confirmed after a multiple phase flashover, and a statistical analysis was conducted to investigate factors affecting the generation of power follow current. These results can serve as a valuable resource to help clarify the mechanisms underlying the production of distribution-line faults caused by lightning effects. [J21]

"Evidence theory-based fake measurement identification and fault-tolerant protection in digital substations"

Protective relay is designed to make a trip decision based on calculation of collected measurements, and thus, the quality of data plays an important role in ensuring the reliability of protective relay. However, abnormity of any part of the data acquisition system (DAS), especially cyber risk, may make the protection system receive fake measurements and misoperate. Besides those efforts spent on the reliability of DAS and cyber security, protective relay itself should be able to tolerate fake measurements and actively minimise the impacts associated with bad data. Based on evidence theory, this study proposes an approach taking advantage of abundant

information in digital substations to identify fake measurements and avoid misoperation of protective relay. When protective relay is prone to misoperate after the analysis of fake measurements from several current transformers (CTs) or voltage transformers (VTs), measurements from other CTs/VTs are rapidly collected to indicate whether there is a real fault in the power system. In this way, misoperation because of fake measurements can be prevented and CTs/VTs providing bad data can also be identified. Simulation tests demonstrate the effectiveness of the proposed approach. [J22]

"Scalable Pattern Matching on Multicore Platform via Dynamic Differentiated Distributed Detection (D)"

Pattern Matching (PM) is a key building block for many emerging network applications. Modern multicore platforms are becoming performance competitive with traditional hardware solutions, which are expensive and hard to adapt to the rapid diversification of Internet applications. However, due to uneven network flow sizes and the need to retain packet order within each flow, traditional parallel processing models using packet flows as the basic unit to partition the workload cannot fully take advantage of multicore platforms' power, exhibiting low CPU utilization and poor scalability with increasing numbers of CPUs or cores. In this paper, we propose a novel parallel inspection model called Dynamic Differentiated Distributed Detection (D4). D4deploys balanced parallel detection by adding one more dimension on PM workload partition. The pattern set is prepartitioned into several subsets so as to distribute the workload of the hot flows across multiple cores while still maintaining packet order within each flow. We also show theoretically that higher number of subsets leads to higher algorithmic overhead. To achieve optimal throughput for all flow size distributions, D4prepartitions the pattern set in several ways for use in different detection modes beforehand, and then, dynamically switches among these modes on-the-fly according to the flow and runtime information it senses. D4also allows multiple PM algorithms to work simultaneously on different pattern subsets. According to several heuristics and the algorithms' characteristics, the detection mode selection and subset partitioning algorithms are designed to maximize the CPU/core utilization while avoiding unnecessary overheads. Experiments show that D4features high core utilization and low overhead, thus achieving distinct performance gains against traditional load balancing schemes, as shown by experimental results using real-world pattern sets and traffi--c traces. [J23]

"Virtualized ECC: Flexible Reliability in Main Memory"

Virtualized error checking and correcting (ECC) is a scheme that virtualizes memory-error correction. Unlike traditional uniform ECC, which provides a fixed level of error tolerance, virtualized ECC enables flexible memory protection by mapping redundant information needed for correcting errors onto the memory namespace. Additionally, virtualized ECC enables error-correction mechanisms that can adapt to user and system demands. [J24]

"Attacks and Defenses for JTAG"

JTAG is a well-known standard mechanism for in-field test. Although it provides high controllability and observability, it also poses great security challenges. This article analyzes various attacks and proposes protection schemes. [J25]

"Robust MAC-lite and soft header recovery for packetized multimedia transmission"

This paper presents an enhanced permeable layer mechanism useful for highly robust packetized multimedia transmission. Packet header recovery at various protocol layers using MAP estimation is the cornerstone of the proposed solution. The inherently available intra-layer and inter-layer header correlation proves to be very effective in selecting a reduced set of possible header configurations for further processing. The best candidate is then obtained through soft decoding of CRC protected data and CRC redundancy information itself. Simulation results for WiFi transmission using DBPSK modulated signals over AWGN channels show a substantial (4 to 12 dB) link budget improvement over classical hard decision procedures. We also introduce a sub-optimal and hardware realizable version of the proposed algorithm. [J26]

"Heredity as an Encoded Communication Process"

Heredity is relevant to information theory as a communication process. The conservation of genomes over intervals at the geological timescale and the existence of mutations at shorter intervals can be conciliated assuming that genomes possess intrinsic error-correction codes. The better conservation of old parts of genomes leads to assume that these codes are organized as a nested system set up during geological times, which protects a genomic message the better, the older it is. These hypotheses imply that: genomes are redundant, discrete species exist with a hierarchical taxonomy, successive generations are needed, evolution is

contingent and saltationist; it trends towards increasing complexity. These consequences match features of the actual living world but their experimental confirmation needs a still lacking collaboration of biologists and information-theorists. It is suggested that genomic error-correcting codes could consist of Г‚Вїsoft codesГ‚Вї where mutual dependence of symbols results from physical-chemical and linguistic constraints, not only mathematical equalities. The constraints incurred by DNA molecules moreover result in a nested structure. Guesses about genomic error-correcting codes are made. [J27]

"Blind Authentication: A Secure Crypto-Biometric Verification Protocol"

Concerns on widespread use of biometric authentication systems are primarily centered around template security, revocability, and privacy. The use of cryptographic primitives to bolster the authentication process can alleviate some of these concerns as shown by biometric cryptosystems. In this paper, we propose a provably secureand blindbiometric authentication protocol, which addresses the concerns of user's privacy, template protection, and trust issues. The protocol is blind in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography. The authentication protocol can run over public networks and provide nonrepudiable identity verification. The encryption also provides template protection, the ability to revoke enrolled templates, and alleviates the concerns on privacy in widespread use of biometrics. The proposed approach makes no restrictive assumptions on the biometric data and is hence applicable to multiple biometrics. Such a protocol has significant advantages over existing biometric cryptosystems, which use a biometric to secure a secret key, which in turn is used for authentication. We analyze the security of the protocol under various attack scenarios. Experimental results on four biometric datasets (face, iris, hand geometry, and fingerprint) show that carrying out the authentication in the encrypted domain does not affect the accuracy, while the encryption key acts as an additional layer of security. [J28]

"Compliance with Information Security Policies: An Empirical Investigation"

Information security was the main topic in this paper. An investigation of the compliance to information security policies were discussed. The author mentions that the insignificant relationship between rewards and actual compliance with information security policies does not make sense. Quite possibly this relationship results from not applying rewards for security compliance. Also mentions that based on the survey conducted, careless employee behavior places an organization's assets and reputation in serious jeopardy. The major threat to information security arises from careless employees who fail to comply with organizations' information security policies and procedures. [J29]

"Privacy-Preserving Collaborative Recommender Systems"

Collaborative recommender systems use various types of information to help customers find products of personalized interest. To increase the usefulness of collaborative recommender systems in certain circumstances, it could be desirable to merge recommender system databases between companies, thus expanding the data pool. This can lead to privacy disclosure hazards during the merging process. This paper addresses how to avoid privacy disclosure in collaborative recommender systems by comparing with major cryptology approaches and constructing a more efficient privacy-preserving collaborative recommender system based on the scalar product protocol. [J30]

"Secure and Robust Error Correction for Physical Unclonable Functions"

Physical unclonable functions (PUFs) offer a promising mechanism that can be used in many security, protection, and digital rights management applications. One key issue is the stability of PUF responses that is often addressed by error correction codes. The authors propose a new syndrome coding scheme that limits the amount of leaked information by the PUF error-correcting codes. [J31]

"Signal Transmission With Unequal Error Protection in Wireless Relay Networks"

This paper studies a relaying technique based on the signal-to-noise (SNR) threshold in cooperative networks using hierarchical modulation. Hierarchical modulation is useful in applications that require different protection classes of the information. In particular, a cooperative network with one source, one relay, and one destination is considered. Two different protection classes are modulated by a hierarchical 2/4-amplitude shift keying (ASK) constellation at the source. Based on the instantaneous received SNR at the relay, the relay decides to retransmit both classes by using a hierarchical 2/4-ASK constellation, or the more-protection class by using a 2-ASK constellation, or remains silent. Optimal thresholds are chosen to minimize the bit error rate (BER) of the less-protection class, whereas the BER of the more-protection class meets a given requirement. Numerical and

simulation results are provided to verify the analysis. The results show that the optimal thresholds significantly improve the performance. [J32]

"A cognitive radio system for e-health applications in a hospital environment"

Wireless communications technologies are used to support a variety of electronic health applications to transfer medical data and patient information. However, using wireless communications technology in a healthcare environment poses two major challenges. First, the electromagnetic interference caused to bio-medical devices by wireless devices could critically affect their performance. Second, since different types of e-health applications have different priorities, access to the wireless channel by the corresponding devices needs to be prioritized. In this article we introduce a novel cognitive-radio-based approach to address these challenges in wireless communications for e-health applications in a hospital environment. First, the requirements for a wireless communications system to be used in a healthcare environment are identified, and potential applications of cognitive radio technology for e-health applications are discussed. Then a cognitive radio system is proposed for e-health applications in a hospital environment, which protects the medical devices from harmful interference by adapting the transmit power of wireless devices based on EMI constraints. An EMI-aware handshaking protocol is proposed for channel access by two different types of applications with different priorities. The performance of this cognitive radio system for e-health applications is evaluated through simulations. [J33]

"Data security and privacy in wireless body area networks"

The wireless body area network has emerged as a new technology for e-healthcare that allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern, with challenges coming from stringent resource constraints of WBAN devices, and the high demand for both security/privacy and practicality/usability. In this article we look into two important data security issues: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. We discuss various practical issues that need to be taken into account while fulfilling the security and privacy requirements. Relevant solutions in sensor networks and WBANs are surveyed, and their applicability is analyzed. [J34]

"Guest Editors' Introduction: Confronting the Hardware Trustworthiness Problem"

The emergence of a globalized, horizontal semiconductor business model raises concerns involving the security and trust of the information systems on which modern society is increasingly reliant for mission-critical functionality. Traditionally, hardware-based security techniques and countermeasures modify hardware to prevent attacks and to protect IP blocks or secret keys. Some of the emerging types of attacks covered by this special issue are fundamentally different: the attacker is assumed to maliciously alter the design before or during fabrication. [J35]

"A New Framework for Adaptive Multimodal Biometrics Management"

This paper presents a new evolutionary approach for adaptive combination of multiple biometrics to ensure the optimal performance for the desired level of security. The adaptive combination of multiple biometrics is employed to determine the optimal fusion strategy and the corresponding fusion parameters. The score-level fusion rules are adapted to ensure the desired system performance using a hybrid particle swarm optimization model. The rigorous experimental results presented in this paper illustrate that the proposed score-level approach can achieve significantly better and stable performance over the decision-level approach. There has been very little effort in the literature to investigate the performance of an adaptive multimodal fusion algorithm on real biometric data. This paper also presents the performance of the proposed approach from the real biometric samples which further validate the contributions from this paper. [J36]

"CAR-2-X and Pedestrian Safety"

Traffic accidents involving pedestrians or cyclists cause thousands of fatalities and serious injuries every year. In this article, we present an innovative approach for a collision avoidance system that seeks to reduce these accidents. We also discuss the different architectural approaches utilizing ad hoc and/or cellular technologies and different processing setups and present a physical analysis of the system time available between detection, warning, and reaction to give an overview of the time constraint. [J37]

"Heart Rate and Accelerometer Data Fusion for Activity Assessment of Rescuers During Emergency Interventions"

The current state of the art in wearable electronics is the integration of very small devices into textile fabrics, the so-called ??smart garment.?? The ProeTEX project is one of many initiatives dedicated to the development of smart garments specifically designed for people who risk their lives in the line of duty such as fire fighters and Civil Protection rescuers. These garments have integrated multipurpose sensors that monitor their activities while in action. To this aim, we have developed an algorithm that combines both features extracted from the signal of a triaxial accelerometer and one ECG lead. Microprocessors integrated in the garments detect the signal magnitude area of inertial acceleration, step frequency, trunk inclination, heart rate (HR), and HR trend in real time. Given these inputs, a classifier assigns these signals to nine classes differentiating between certain physical activities (walking, running, moving on site), intensities (intense, mild, or at rest) and postures (lying down, standing up). Specific classes will be identified as dangerous to the rescuer during operation, such as, ?? subject motionless lying down?? or ??subject resting with abnormal HR.?? Laboratory tests were carried out on seven healthy adult subjects with the collection of over 4.5 h of data. The results were very positive, achieving an overall classification accuracy of 88.8%. [J38]

"Pedestrian Detection and Tracking in an Urban Environment Using a Multilayer Laser Scanner"

Pedestrians are the most vulnerable participants in urban traffic. The first step toward protecting pedestrians is to reliably detect them in a real-time framework. In this paper, a new approach is presented for pedestrian detection in urban traffic conditions using a multilayer laser sensor mounted onboard a vehicle. This sensor, which is placed on the front of a vehicle, collects information about the distance distributed according to four planes. Like a vehicle, a pedestrian constitutes, in the vehicle environment, an obstacle that must be detected, and located and then identified and tracked if necessary. To improve the robustness of pedestrian detection using a single laser sensor, a detection system based on the fusion of information located in the four laser planes is proposed. The method uses a nonparametric kernel-density-based estimation of pedestrian position of each laser plane. The resulting pedestrian estimations are then sent to a decentralized fusion according to the four planes. Temporal filtering of each object is finally achieved within a stochastic recursive Bayesian framework (particle filter), allowing a closer observation of pedestrian random movement dynamics. Many experimental results are given and validate the relevance of our pedestrian-detection algorithm with regard to a method using only a single-row laser-range scanner. [J39]

"Smart Garments for Emergency Operators: The ProeTEX Project"

Financed by the European Commission, a consortium of 23 European partners, consisting of universities, research institutions, industries, and organizations operating in the field of emergency management, is developing a new generation of ??smart?? garments for emergency-disaster personnel. Garments integrate newly developed wearable and textile solutions, such as commercial portable sensors and devices, in order to continuously monitor risks endangering rescuers' lives. The system enables detection of health-state parameters of the users (heart rate, breathing rate, body temperature, blood oxygen saturation, position, activity, and posture) and environmental variables (external temperature, presence of toxic gases, and heat flux passing through the garments), to process data and remotely transmit useful information to the operation manager. The European-integrated project, called ProeTEX (Protection e-Textiles: Micro-Nano-Structured fiber systems for Emergency-Disaster Wear) started on February, 2006 and will end on July, 2010. During this 4.5 years period, three subsequent generations of sensorized garments are being released. This paper proposes an overview of the project and gives a description of the second-generation prototypes, delivered at the end of 2008. [J40]

"Multilevel Modulation for Cognitive Multiaccess Relay Channel"

In this paper, we propose a simple protocol for the cognitive multiaccess relay channel (MARC) with no transmit channel-state information and analyze the resulting stable throughputs of the primary and cognitive nodes. We propose allowing the cognitive node (common relay in the MARC topology) to simultaneously relay data for both primary nodes and transmit its own data (cognitive data) using a multilevel modulation (MLM) scheme. This modulation scheme provides unequal protection for the primary and cognitive data, which increases the throughput of the primary nodes by relaying their messages, in turn increasing the transmission opportunities of the cognitive nodes. The proposed scheme is studied from a networking perspective, and the stable throughput for the primary and secondary nodes as a function of the modulation levels and channel statistics is derived using queueing theory. [J41]

"Smart Transmission Grid Applications and Their Supporting Infrastructure"

In this paper we assume that time synchronized measurements will be ubiquitously available at all high-voltage substations at very high rates. We examine how this information can be utilized more effectively for real-time operation as well as for subsequent decision making. This new information available in real time is different, both in quality and in quantity, than the real-time measurements available today. The promise of new and improved applications to operate the power system more reliably and efficiently has been recognized but is still in conceptual stages. Also, the present system to handle this real-time data has been recognized to be inadequate but even conceptual designs of such infrastructure needed to store and communicate the data are in their infancy. In this paper, we first suggest the requirements for an information infrastructure to handle ubiquitous phasor measurements recognizing that the quantity and rate of data would make it impossible to store all the data centrally as done today. Then we discuss the new and improved applications, classified into two categories: one is the set of automatic wide-area controls and the other is the set of control center (EMS) functions with special attention to the state estimator. Finally, given that the availability of phasor measurements will grow over time, the path for smooth transition from present-day systems and applications to those discussed here is delineated. [J42]

"Variations on Information Embedding in Multiple Access and Broadcast Channels"

Information embedding (IE) is the transmission of information within a host signal subject to a distortion constraint. There are two types of embedding methods, namely irreversible IE and reversible IE, depending upon whether or not the host, as well as the message, is recovered at the decoder. In irreversible IE, only the embedded message is recovered at the decoder, and in reversible IE, both the message and the host are recovered at the decoder. In this paper, combinations of irreversible and reversible IE in multiple access channels (MAC) and physically degraded broadcast channels (BC) are considered. In this paper, MAC IE in which separate encoders embed their messages into their host signals subject to distortion constraints is considered. The embedded signals from the two encoders are transmitted to a single decoder across a MAC. For the MAC IE model, the following three cases are considered: A) no host recovery at the decoder, B) lossless recovery of one host at the decoder, and C) lossless recovery of both hosts at the decoder. For the cases A and B, inner bounds on the respective capacity regions are developed. For the case C, inner and outer bounds on the capacity region are developed, and the capacity region is obtained if the hosts are independent. In this paper, BC IE in which two messages intended for separate decoders are embedded into a given host sequence by a single encoder subject to a distortion constraint is also considered. For the BC IE model, the following four cases are considered: A') lossless recovery of the host sequence at neither of the decoders, B') lossless recovery of the host sequence at only the better decoder, C') lossless recovery of the host sequence at both decoders, and D') lossless recovery of the host sequence at only the worse decoder. For cases A' and B', inner and outer bounds on the respective capacity regions are developed. For cases C' and D', the identical capacity regions are obtained. [J43]

"Optimal PET Protection for Streaming Scalably Compressed Video Streams With Limited Retransmission Based on Incomplete Feedback"

For streaming scalably compressed video streams over unreliable networks, Limited-Retransmission Priority Encoding Transmission (LR-PET) outperforms PET remarkably since the opportunity to retransmit is fully exploited by hypothesizing the possible future retransmission behavior before the retransmission really occurs. For the retransmission to be efficient in such a scheme, it is critical to get adequate acknowledgment from a previous transmission before deciding what data to retransmit. However, in many scenarios, the presence of a stochastic packet delay process results in frequent late acknowledgments, while imperfect feedback channels can impare the server's knowledge of what the client has received. This paper proposes an extended LR-PET scheme, which optimizes PET-protection of transmissed bitstreams, recognizing that the received feedback information is likely to be incomplete. Similar to the original LR-PET, the behavior of future retransmissions is hypothesized in the optimization objective of each transmission opportunity. As the key contribution, we develop a method to efficiently derive the effective recovery probability versus redundancy rate characteristic for the extended LR-PET communication process. This significantly simplifies the ultimate protection assignment procedure. This paper also demonstrates the advantage of the proposed strategy over several alternative strategies. [J44]

"An Intelligent Telecardiology System Using a Wearable and Wireless ECG to Detect Atrial Fibrillation"

This study presents a novel wireless, ambulatory, real-time, and autoalarm intelligent telecardiology system to improve healthcare for cardiovascular disease, which is one of the most prevalent and costly health problems in the world. This system consists of a lightweight and power-saving wireless ECG device equipped with a built-in automatic warning expert system. This device is connected to a mobile and ubiquitous real-time display platform.

The acquired ECG signals are instantaneously transmitted to mobile devices, such as netbooks or mobile phones through Bluetooth, and then, processed by the expert system. An alert signal is sent to the remote database server, which can be accessed by an Internet browser, once an abnormal ECG is detected. The current version of the expert system can identify five types of abnormal cardiac rhythms in real-time, including sinus tachycardia, sinus bradycardia, wide QRS complex, atrial fibrillation (AF), and cardiac asystole, which is very important for both the subjects who are being monitored and the healthcare personnel tracking cardiac-rhythm disorders. The proposed system also activates an emergency medical alarm system when problems occur. Clinical testing reveals that the proposed system is approximately 94% accurate, with high sensitivity, specificity, and positive prediction rates for ten normal subjects and 20 AF patients. We believe that in the future a business-card-like ECG device, accompanied with a mobile phone, can make universal cardiac protection service possible. [J45]

"PIPWatch Toolbar: Using Social Navigation to Enhance Privacy Protection and Compliance"

The main goal of this project is to evaluate the prospects of combining social navigation techniques into a PET that helps Internet users identify which Websites comply with Canadian privacy legislation and to honor the concerns common among Canadians who conduct personal transactions via the Web. Our PIPWatch tool allows users to collect and share information about the privacy practices of various Websites. [J46]

"Path Computation Algorithms for Dynamic Service Provisioning With Protection and Inverse Multiplexing in SDH/SONET Networks"

Synchronous Digital Hierarchy (SDH) and Synchronous Optical Network (SONET) are time-division multiplexing technologies widely used in transport networks to provide bandwidth services. Dynamic service provisioning requires the use of online algorithms that automatically compute the path to be taken to satisfy the given service request. SDH/SONET multiplexing structure imposes restrictions on the allocation of bandwidth. Bandwidth services mostly require protection so that they are resilient to failures in the network. Two types of protection techniques-namely, dedicated protection and shared protection-are commonly used to protect bandwidth. Also, SDH/SONET provides standard protection mechanisms like linear MSP/APS, MS-SPRing/BLSR and SNCP/UPSR. In shared protection, complete path information for all the existing connections has to be maintained to maximize sharing for future service requests. This information will be typically very large. To overcome this problem, a minimum information scenario is proposed as a tradeoff between maintaining less information and maximizing sharing. In this work, heuristic algorithms are proposed for dedicated and shared protection that take into account the above-mentioned factors. These algorithms use the path computation algorithms for SDH networks proposed in a previous work of the authors, which compute paths for service requests without considering protection. The performance is evaluated for different values for the relative weight of sharing for the complete and minimum information scenarios. An extension to these algorithms for satisfying bandwidth requests that use various inverse multiplexing techniques is also proposed. [J47]

"Gate-Level Information-Flow Tracking for Secure Architectures"

This article describes a new method for constructing and analyzing architectures that can track all information flows within a processor, including explicit, implicit, and timing flows. The key to this approach is a novel gate-level information-flow-tracking method that provides a way to create complex logical structures with well-defined information-flow properties. [J48]

"Codes for Asymmetric Limited-Magnitude Errors With Application to Multilevel Flash Memories"

Several physical effects that limit the reliability and performance of multilevel flash memories induce errors that have low magnitudes and are dominantly asymmetric. This paper studies block codes for asymmetric limited-magnitude errors over q-ary channels. We propose code constructions and bounds for such channels when the number of errors is bounded by tand the error magnitudes are bounded by l. The constructions utilize known codes for symmetric errors, over small alphabets, to protect large-alphabet symbols from asymmetric limited-magnitude errors. The encoding and decoding of these codes are performed over the small alphabet whose size depends only on the maximum error magnitude and is independent of the alphabet size of the outer code. Moreover, the size of the codes is shown to exceed the sizes of known codes (for related error models), and asymptotic rate-optimality results are proved. Extensions of the construction are proposed to accommodate variations on the error model and to include systematic codes as a benefit to practical implementation. [J49]

"A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems"

Nowadays, critical control systems are a fundamental component contributing to the overall performance of critical infrastructures in our society, most of which belong to the industrial sector. These complex systems

include in their design different types of information and communication technology systems, such as wireless (mesh) sensor networks, to carry out control processes in real time. This fact has meant that several communication standards, such as Zigbee PRO, WirelessHART, and ISA100.11a, have been specified to ensure coexistence, reliability, and security in their communications. The main purpose of this paper has been to review these three standards and analyze their security. We have identified a set of threats and potential attacks in their routing protocols, and we consequently provide recommendations and countermeasures to help Industry protect its infrastructures. [J50]

"The Limits of Notice and Choice"

The US Federal Trade Commission (FTC) has embarked on a series of three workshops on exploring privacy. The first, in December 2009 in Washington, DC, focused on market and regulatory issues; the second, in January in Berkeley, California, examined technological issues; and the third, scheduled for March in Washington again, will focus on possible solutions. But after hearing from more than 70 speakers at two standing-room only workshops, at least one theme is emerging: notice and choice are inadequate tools for protecting information privacy or security. [J51]

"My Information, Your Code"

Modern file formats provide great flexibility to users and system designers to interact with computers in completely new ways. Unfortunately, the very flexibility the users are embracing is also the greatest threat to modern enterprises. [J52]

"Comparative Evaluation of Susceptibility to Motion Artifact in Different Wearable Systems for Monitoring Respiratory Rate"

The purpose of this study is to comparatively evaluate the performance of different wearable systems based on indirect breathing monitoring in terms of susceptibility to motion artifacts. These performances are compared with direct respiratory measurements using a spirometer, which is accurate, reliable, and less sensitive to movement artifacts, but cannot be integrated into truly wearable form. Experiments were carried out on four indirect methods implemented into wearable systems, inductive plethysmography, impedance plethysmography, piezoresistive pneumography, and piezoelectric pneumography, to ascertain the performance of each of them in terms of noise due to movement artifacts, as well as to study the effects of different movements or gestures during each test. A group of volunteers was asked to wear all of the breath monitoring systems simultaneously along with the face mask of the spirometer while carrying out four physical exercises in a gym under controlled conditions. Data are analyzed in the time and frequency domain to estimate the frequency respiration from each wearable system and compare it with those of the spirometer. Results confirmed that all the wearable systems are somehow affected by movement artifacts, but statistical investigation showed that for most of the physical exercises, three out of four, piezoelectric pneumography provided best performance in terms of robustness and reduced susceptibility to movement artifacts. [J53]

"Hierarchical Segmentation of R&D Process and Intellectual Property Protection: Evidence From Multinational R&D Laboratories in China"

This paper examines how multinational corporations (MNCs) protect their intellectual property (IP) when they conduct R&D in countries with weak IP rights (IPRs) protection. Findings from a small-scale survey and three case studies in China show that hierarchical segmentation of the R&D process can provide an effective way for IPR protection. Furthermore, a modular R&D structure adopted by many information technology companies can facilitate the hierarchical segmentation. Because R&D is becoming distributed across locations with varying levels of IPR protection, a center-peripheral R&D organizational structure is emerging within MNCs as R&D globalization proceeds. [J54]

"An Analytic Model-Based Approach for Power System Alarm Processing Employing Temporal Constraint Network"

The alarm-processing problem is to interpret a large number of alarms under stress conditions, such as faults or disturbances, by providing summarized and synthesized information instead of a flood of raw alarm data. Alarm timestamps represent the temporal relationship among event occurrences and consist of rich and useful information for alarm processing. However, the temporal information has not been well utilized in existing alarm-processing methods. The temporal constraint network (TCN) is a type of directed acyclic graph suitable for representing temporal logics. Based on TCN, a new analytic model is developed for alarm processing with temporal information taken into account. Three major modules are included in the developed approach or alarm

processor (i.e., alarm selection, event analysis, and result evaluation). In the alarm selection module, reported alarms are divided into related groups. The function of the event analysis module is to find out what events cause the reported alarms and to estimate when these events happen. The result evaluation module is used to identify abnormal or missing alarms. Finally, two alarm-processing scenarios of an actual power system are served for demonstrating the feasibility and efficiency of the developed approach. [J55]

"On Unequal Error Protection of Convolutional Codes From an Algebraic Perspective"

In this paper, convolutional codes are studied for unequal error protection (UEP) from an algebraic theoretical viewpoint. We first show that for every convolutional code there exists at least one optimal generator matrix with respect to UEP. The UEP optimality of convolutional encoders is then combined with several algebraic properties, e.g., systematic, basic, canonical, and minimal, to establish the fundamentals of convolutional codes for UEP. In addition, a generic lower bound on the length of a UEP convolutional code is proposed. Good UEP codes with their lengths equal to the derived lower bound are obtained by computer search. [J56]

"A Hybrid Approach for Generating Secure and Discriminating Face Template"

Biometric template protection is one of the most important issues in deploying a practical biometric system. To tackle this problem, many algorithms, that do not store the template in its original form, have been reported in recent years. They can be categorized into two approaches, namely biometric cryptosystem and transform-based. However, most (if not all) algorithms in both approaches offer a trade-off between the template security and matching performance. Moreover, we believe that no single template protection method is capable of satisfying the security and performance simultaneously. In this paper, we propose a hybrid approach which takes advantage of both the biometric cryptosystem approach and the transform-based approach. A three-step hybrid algorithm is designed and developed based on random projection, discriminability-preserving (DP) transform, and fuzzy commitment scheme. The proposed algorithm not only provides good security, but also enhances the performance through the DP transform. Three publicly available face databases, namely FERET, CMU-PIE, and FRGC, are used for evaluation. The security strength of the binary templates generated from FERET, CMU-PIE, and FRGC databases are 206.3, 203.5, and 347.3 bits, respectively. Moreover, noninvertibility analysis and discussion on data leakage of the proposed hybrid algorithm are also reported. Experimental results show that, using Fisherface to construct the input facial feature vector (face template), the proposed hybrid method can improve the recognition accuracy by 4%, 11%, and 15% on the FERET, CMU-PIE, and FRGC databases, respectively. A comparison with the recently developed random multispace quantization biohashing algorithm is also reported. [J57]

"Participatory sensing: applications and architecture [JInternet Predictions]"

Participatory sensing is the process whereby individuals and communities use ever more capable mobile phones and cloud services to collect and analyze systematic data for use in discovery. The convergence of technology and analytical innovation with a citizenry that is increasingly comfortable using mobile phones and online social networking sets the stage for this technology to dramatically impact many aspects of daily lives. Ubiquitous data capture, leveraged data processing, and personal data vault are the essential components for these emerging systems. The architecture, usage models,and application of participatory sensing were discussed in this paper. [J58]

"Internet predictions [JGuest editor's introduction]"

More than a dozen leading experts give their opinions on where the Internet is headed and where it will be in the next decade in terms of technology, policy, and applications. They cover topics ranging from the Internet of Things to climate change to the digital storage of the future. [J59]

"Using Web-Referral Architectures to Mitigate Denial-of-Service Threats"

The web is a complicated graph, with millions of websites interlinked together. In this paper, we propose to use this web sitegraph structure to mitigate flooding attacks on a website, using a new web referral architecture for privileged service ("WRAPS"). WRAPS allows a legitimate client to obtain a privilege URL through a simple click on a referral hyperlink, from a website trusted by the target website. Using that URL, the client can get privileged access to the target website in a manner that is far less vulnerable to a distributed denial-of-service (DDoS) flooding attack than normal access would be. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which makes its deployment easy. The massive scale of the web sitegraph could deter attempts to isolate a website through blocking all referrers. We present the design of WRAPS, and the implementation of a prototype system used to evaluate our proposal. Our empirical study demonstrates that WRAPS enables legitimate clients to connect to a website smoothly in spite of a very

intensive flooding attack, at the cost of small overheads on the website's ISP's edge routers. We discuss the security properties of WRAPS and a simple approach to encourage many small websites to help protect an important site during DoS attacks. [J60]

"Multisensor and Multitemporal Fusion of VHR Satellite Imagery Based on KIM"

Similar to many advanced approaches in multisensor image analysis, image information mining (IIM) is hampered by sensor-specific differences in spatial resolution and spectral response. This study examines the representation of semantic categories integrating Ikonos and Quickbird imagery in the knowledge-based information mining system KIM. A processing sequence is presented, which accounts for sensor-related differences along with an evaluation of the application of IIM technologies in operational rapid-mapping scenarios. [J61]

"Survey of Pedestrian Detection for Advanced Driver Assistance Systems"

Advanced driver assistance systems (ADASs), and particularly pedestrian protection systems (PPSs), have become an active research area aimed at improving traffic safety. The major challenge of PPSs is the development of reliable on-board pedestrian detection systems. Due to the varying appearance of pedestrians (e.g., different clothes, changing size, aspect ratio, and dynamic shape) and the unstructured environment, it is very difficult to cope with the demanded robustness of this kind of system. Two problems arising in this research area are the lack of public benchmarks and the difficulty in reproducing many of the proposed methods, which makes it difficult to compare the approaches. As a result, surveying the literature by enumerating the proposals one--after-another is not the most useful way to provide a comparative point of view. Accordingly, we present a more convenient strategy to survey the different approaches. We divide the problem of detecting pedestrians from images into different processing steps, each with attached responsibilities. Then, the different proposed methods are analyzed and classified with respect to each processing stage, favoring a comparative viewpoint. Finally, discussion of the important topics is presented, putting special emphasis on the future needs and challenges. [J62]

"Spectral Anonymization of Data"

The goal of data anonymization is to allow the release of scientifically useful data in a form that protects the privacy of its subjects. This requires more than simply removing personal identifiers from the data because an attacker can still use auxiliary information to infer sensitive individual information. Additional perturbation is necessary to prevent these inferences, and the challenge is to perturb the data in a way that preserves its analytic utility. No existing anonymization algorithm provides both perfect privacy protection and perfect analytic utility. We make the new observation that anonymization algorithms are not required to operate in the original vector-space basis of the data, and many algorithms can be improved by operating in a judiciously chosen alternate basis. A spectral basis derived from the data's eigenvectors is one that can provide substantial improvement. We introduce the term spectral anonymization to refer to an algorithm that uses a spectral basis for anonymization, and give two illustrative examples. We also propose new measures of privacy protection that are more general and more informative than existing measures, and a principled reference standard with which to define adequate privacy protection. [J63]

"Snoogle: A Search Engine for Pervasive Environments"

Embedding small devices into everyday objects like toasters and coffee mugs creates a wireless network of objects. These embedded devices can contain a description of the underlying objects, or other user defined information. In this paper, we present Snoogle, a search engine for such a network. A user can query Snoogle to find a particular mobile object, or a list of objects that fit the description. Snoogle uses information retrieval techniques to index information and process user queries, and Bloom filters to reduce communication overhead. Security and privacy protections are also engineered into Snoogle to protect sensitive information. We have implemented a prototype of Snoogle using off-the-shelf sensor motes, and conducted extensive experiments to evaluate the system performance. [J64]

"In-Depth Packet Inspection Using a Hierarchical Pattern Matching Algorithm"

Detection engines capable of inspecting packet payloads for application-layer network information are urgently required. The most important technology for fast payload inspection is an efficient multipattern matching algorithm, which performs exact string matching between packets and a large set of predefined patterns. This paper proposes a novel Enhanced Hierarchical Multipattern Matching Algorithm (EHMA) for packet inspection. Based on the occurrence frequency of grams, a small set of the most frequent grams is discovered and used in the EHMA. EHMA is a two-tier and cluster-wise matching algorithm, which significantly reduces the amount of

external memory accesses and the capacity of memory. Using a skippable scan strategy, EHMA speeds up the scanning process. Furthermore, independent of parallel and special functions, EHMA is very simple and therefore practical for both software and hardware implementations. Simulation results reveal that EHMA significantly improves the matching performance. The speed of EHMA is about 0.89-1,161 times faster than that of current matching algorithms. Even under real-life intense attack, EHMA still performs well. [J65]

"Detecting Intrusions through System Call Sequence and Argument Analysis"

We describe an unsupervised host-based intrusion detection system based on system call arguments and sequences. We define a set of anomaly detection models for the individual parameters of the call. We then describe a clustering process that helps to better fit models to system call arguments and creates interrelations among different arguments of a system call. Finally, we add a behavioral Markov model in order to capture time correlations and abnormal behaviors. The whole system needs no prior knowledge input; it has a good signal-to-noise ratio, and it is also able to correctly contextualize alarms, giving the user more information to understand whether a true or false positive happened, and to detect global variations over the entire execution flow, as opposed to punctual ones over individual instances. [J66]

"Shifting Inference Control to User Side: Architecture and Protocol"

Inference has been a longstanding issue in database security, and inference control, aiming to curb inference, provides an extra line of defense to the confidentiality of databases by complementing access control. However, in traditional inference control architecture, database server is a crucial bottleneck, as it enforces highly computation-intensive auditing for all users who query the protected database. As a result, most auditing methods, though rigorously studied, are not practical for protecting large-scale real-world database systems. In this paper, we shift this paradigm by proposing a new inference control architecture, entrusting inference control to each user's platform that is equipped with trusted computing technology. The trusted computing technology is designed to attest the state of a user's platform to the database server, so as to assure the server that inference control could be enforced as prescribed. A generic protocol is proposed to formalize the interactions between the user's platform and database server. The authentication property of the protocol is formally proven. Since inference control is enforced in a distributed manner, our solution avoids the bottleneck in the traditional architecture, thus can potentially support a large number of users making queries. [J67]

"Secure Client-Side ST-DM Watermark Embedding"

Client-side watermark embedding systems have been proposed as a possible solution for the copyright protection in large-scale content distribution environments. In this framework, we propose a new look-up-table-based secure client-side embedding scheme properly designed for the spread transform dither modulation watermarking method. A theoretical analysis of the detector performance under the most known attack models is presented and the agreement between theoretical and experimental results verified through several simulations. The experimental results also prove that the advantages of the informed embedding technique in comparison to the spread-spectrum watermarking approach, which are well known in the classical embedding schemes, are preserved in the client-side scenario. The proposed approach permits us to successfully combine the security of client-side embedding with the robustness of informed embedding methods. [J68]

"Women in Cybersecurity: A Study of Career Advancement"

Although cybersecГ‚Вїrity is a critical IT area, women continue to be underrepresented among its ranks. This first study of female cybersecurity professionals examines the required skills, existing challenges, and key success factors for women in the field.As our results show, addressing the needs of women at the beginning of their careers-starting at educational institutions-is crucial to their successful entry and success in the field.Currently, the US government has responded to this issue by providing grants to attract and train women in cybersecurity at the university level. [J69]

"Inferring Personal Information from Demand-Response Systems"

Current and upcoming demand-response systems provide increasingly detailed power-consumption data to utilities and a growing array of players angling to assist consumers in understanding and managing their energy use. The granularity of this data, as well as new players' entry into the energy market, creates new privacy concerns. The detailed per-household consumption data that advanced metering systems generate reveals information about in-home activities that such players can mine and combine with other readily available information to discover more about occupants' activities. The authors explore the technological aspects of this claim, focusing on the ways in which personally identifying information can be collected and repurposed. Their results show that, even with relatively unsophisticated hardware and data-extraction algorithms, some

information about occupant behavior can be estimated with a high degree of accuracy. The authors propose a disclosure metric to aid in quantifying the impact of data collection on in-home privacy and construct an example metric for their experiment. [J70]

"Message Origin Authentication and Integrity Protection in Chaos-Based Optical Communication"

In this paper, a message authentication and integrity protection scheme based on optically generated chaos is proposed. The introduced protocol relies physically on the dependence of chaos synchronization on the phase experienced by the delayed portion of the optical field inside the external cavity. The protocol's security is analytically evaluated, considering data modification and impersonation attack scenarios, and issues related to the practical implementation of the scheme are investigated. [J71]

"Joint sensing time and power allocation in cooperatively cognitive networks"

The jointly optimal allocation of sensing time and power for a two-user amplify-and-forward overlay cognitive network is developed by maximizing the averaged aggregate throughput of the secondary network. In particular, observing that the sensing duration lies within a strict interval, the jointly optimal strategy of sensing time and power allocation is proved to be tractable by sequential optimization. [J72]

"2PASS: Bandwidth-Optimized Location Cloaking for Anonymous Location-Based Services"

Protection of users' location privacy is a critical issue for location-based services. Location cloaking has been proposed to blur users' accurate locations with cloaked regions. Although various cloaking algorithms have been studied, none of the prior work has explored the impact of cloaking on the bandwidth usage of requested services. In this paper, we develop an innovative result-aware location cloaking approach, called 2PASS. Based on the notion of Voronoi cells, 2PASS minimizes the number of objects to request, and hence, the bandwidth while meeting the same privacy requirement. The core component of 2PASS is a lightweight WAG-tree index, based on which efficient and secure client and server procedures are designed. Through threat analysis and experimental results, we argue that 2PASS is robust and outperforms state-of-the-art approaches in terms of various metrics, such as query response time and bandwidth consumption. We also enclose a case study of 2PASS in a real-life application. [J73]

"Method for Determining Selective Capability of Current-Limiting Overcurrent Devices Using Peak Let-Through Current-What Traditional Time-Current Curves Will Not Tell You"

Time-current curves are the accepted industry standard for predicting overcurrent device operation and analyzing selective behavior under overload or fault conditions. A conservative interpretation of drawn curves has sufficed for many years and provided acceptable performance. However, recent emphasis on better selectivity while still trying to provide optimal protection increases the demand for more accurate selectivity predictions. Currently, manufacturers are publishing tables and other guidelines to facilitate the selection of optimally coordinated devices by systems designers. However, no standard or single methodology exists for the creation of these tables. The writers shall present three methods of device interaction analysis based on peak let-through current, suitable for predicting selective behavior of protective devices above what time current curves may indicate. The method may be applied with published information or manufacturer's internal test information. [J74]

"Selectivity Analysis in Low-Voltage Power Distribution Systems With Fuses and Circuit Breakers"

Interest in complete overcurrent device selectivity has increased due to the addition of selectivity requirements to articles 700, 701, and 708 of the National Electrical Code (NFPA 70). Many users, both commercial and industrial, use fuses and circuit breakers simultaneously. Traditional time-current curve (TCC) analysis is known to not fully communicate fuse selectivity; hence, fuse manufacturers publish device ratio guidelines for selection of fuse types and sizes. Recent publications of selectivity tables by circuit manufacturers also demonstrate that traditional TCCs are often insufficient to fully communicate circuit breaker selectivity. Traditional TCCs can lead to incorrect conclusions regarding circuit breaker fuse selectivity, indicating more or less selectivity than may be possible. The authors will describe various methods for the assessment of selectivity in systems using both fuses and circuit breakers together, with either device on the line side. The methods will demonstrate that selectivity above what TCCs demonstrate may be possible if devices are selected correctly and that traditional TCC analysis can also incorrectly demonstrate more selectivity than a more thorough analysis would predict. The methods lend themselves to analysis that a power system engineer can perform with published information or information that may be requested from manufacturers. [J75]

"R&D Team's Competencies, Innovation, and Growth With Knowledge Information Flow"

This paper analyzes the interaction among the step-by-step innovation, the product market competition (PMC), and the knowledge information flow in the growth process. Patents protect their holders from being imitated or copied but do not protect them against the possibility that less-efficient competitors master the diffused knowledge. The degree to which diffused knowledge should be exploited by less-efficient firms is determined by both their knowledge assimilating capacities and Research and Development (R&D) teams' competence type and level. The individual skill distribution in R&D team may lead to different innovative behaviors: replicating the knowledge or creation of novel knowledge. Here, we first find that replicating the knowledge and creation of novel knowledge are both growth enhancing; second, the more the flexibility on individual creativity in R&D team is, the faster is the growth; third, the knowledge information flow has a polarization effect on firms' innovative performance. [J76]

"Protecting Coherence and Entanglement by Quantum Feedback Controls"

When a quantum system interacts with its environment, the so-called decoherence effect will normally destroy the coherence in the quantum state and the entanglement between its subsystems. We propose a feedback control strategy based on quantum weak measurements to protect coherence and entanglement of the quantum state against environmental disturbance. For a one-qubit quantum system under amplitude damping and dephasing decoherence channels, our strategy can preserve the coherence based on the measured information about the population difference between its two levels. For a two-qubit quantum system disentangled by independent amplitude damping and dephasing decoherence channels, the designed feedback control can preserve coherence between the ground state and the highest excited states by tuning the coupling strength between the two qubits, and at the same time minimize the loss of entanglement between the two qubits. As a consequence of dynamic symmetry, the generalization of these results derives the concept of control-induced decoherence-free observable subspace, for which several criteria are provided. [J77]

"An Analysis of Random Projection for Changeable and Privacy-Preserving Biometric Verification"

Changeability and privacy protection are important factors for widespread deployment of biometrics-based verification systems. This paper presents a systematic analysis of a random-projection (RP)-based method for addressing these problems. The employed method transforms biometric data using a random matrix with each entry an independent and identically distributed Gaussian random variable. The similarity- and privacy-preserving properties, as well as the changeability of the biometric information in the transformed domain, are analyzed in detail. Specifically, RP on both high-dimensional image vectors and dimensionality-reduced feature vectors is discussed and compared. A vector translation method is proposed to improve the changeability of the generated templates. The feasibility of the introduced solution is well supported by detailed theoretical analyses. Extensive experimentation on a face-based biometric verification problem shows the effectiveness of the proposed method. [J78]

"Lightning Data Observed With Lightning Location System in Portugal"

This paper presents an investigation into cloud-to-ground lightning activity over the continental territory of Portugal with data collected by the National Lightning Location System. The lightning location system in Portugal is first presented. Analyses about geographical, seasonal, and polarity distribution of cloud-to-ground lightning activity and cumulative probability of peak current are carried out. An overall ground flash density map is constructed from the database, which contains the information of more than five years and almost four million records. This map is compared with the thunderstorm days map, produced by the Portuguese Institute of Meteorology, and with the orographic map of Portugal. Finally, conclusions are duly drawn. [J79]

"Advances in vehicular communications networks [JGuest Editorial]"

The articles in this special issue focus on advances in vehicular communications networks. The first four deal with the refinement of several different important mechanisms in vehicular communication protocols, with the aim of controlling and reducing the overall network offered load, while guaranteeing a good level of accuracy, efficiency, and security. The last article proposes a system architecture, called VISIONS, that makes use of the 3G network to disseminate control information. The control information helps routing protocols improve their route selections. [J80]

"Silver Bullet Security Podcast series"

{no data available} [J81]

"Anonymous Multireceiver Identity-Based Encryption"

Recently, many multireceiver identity-based encryption schemes have been proposed in the literature. However, none can protect the privacy of message receivers among these schemes. In this paper, we present an anonymous multireceiver identity-based encryption scheme where we adopt Lagrange interpolating polynomial mechanisms to cope with the above problem. Our scheme makes it impossible for an attacker or any other message receiver to derive the identity of a message receiver such that the privacy of every receiver can be guaranteed. Furthermore, the proposed scheme is quite receiver efficient since each of the receivers merely needs to perform twice of pairing computation to decrypt the received ciphertext. We prove that our scheme is secure against adaptive chosen plaintext attacks and adaptive chosen ciphertext attacks. Finally, we also formally show that every receiver in the proposed scheme is anonymous to any other receiver. [J82]

"Resilient secure aggregation for vehicular networks"

Innovative ways to use ad hoc networking between vehicles are an active research topic and numerous proposals have been made for applications that make use of it. Due to the bandwidth-limited wireless communication medium, scalability is one crucial factor for the success of these future protocols. Data aggregation is one solution to accomplish such scalability. The goal of aggregation is to semantically combine information and only disseminate this combined information in larger regions. However, the integrity of aggregated information cannot be easily verified anymore. Thus, attacks are possible resulting in lower user acceptance of applications using aggregation or, even worse, in accidents due to false information crafted by a malicious user. Therefore, it is necessary to design novel mechanisms to protect aggregation techniques. However, high vehicle mobility, as well as tight bandwidth constraints, pose strong requirements on the efficiency of such mechanisms. We present new security mechanisms for semantic data aggregation that are suitable for use in vehicular ad hoc networks. Resilience against both malicious users of the system and wrong information due to faulty sensors are taken into consideration. The presented mechanisms are evaluated with respect to their bandwidth overhead and their effectiveness against possible attacks. [J83]

"Steering Dynamic Collaborations Between Business Processes"

Under the background of business globalization nowadays, many organizations are connecting their business processes into complex collaborative business processes to facilitate business collaboration. To adapt to the changing requirements and market opportunities, collaborative business processes have to evolve all the time. Such dynamics brings challenges to the modeling and tracking of collaborative business processes. In addition, these issues can be further complicated by the requirements of privacy protection and information openness in the interorganizational context. Aiming to tackle these problems, this paper proposes a comprehensive framework to model and track dynamic collaborative business processes with our extended relative workflow model. This framework helps each participating organization derive its collaborative business processes and update the processes at run time. A process visibility control mechanism is developed to enforce such derivation and extend organizations' process perception via process visibility transitivity. The whole framework is formalized with matrices and is theoretically proven to be privacy safe. Corresponding algorithms are developed for generating and tracking collaborative business processes. A prototype is also implemented for the proof-of-concept purpose. [J84]

"Application of Classical Hermitian Self-Orthogonal MDS Codes to Quantum MDS Codes"

In this paper, we first construct several classes of classical Hermitian self-orthogonal maximum distance separable (MDS) codes. Through these classical codes, we are able to obtain various quantum MDS codes. It turns out that many of our quantum codes are new in the sense that the parameters of our quantum codes cannot be obtained from all previous constructions. [J85]

"A Provably Secure Anonymous Buyer-Seller Watermarking Protocol"

Buyer-seller watermarking (BSW) protocols allow copyright protection of digital content. The protocol is anonymous when the identity of buyers is not revealed if they do not release pirated copies. Existing BSW protocols are not provided with a formal analysis of their security properties. We employ the ideal-world/real-world paradigm to propose a formal security definition for copyright protection protocols, and we analyze an anonymous BSW protocol and prove that it fulfills our definition. Additionally, we implement the protocol and measure its efficiency. [J86]

"SCC18 Updates [JStandards]"

In the July/August 2009 issue of IEEE Industry Applications Magazine, I talked about the IEEE Standards Association (SA), as it relates to other standards-making organizations, namely, the National Fire Protection Association (NFPA) through Standards Coordinating Committee 18 (SCC18). I also provided some information

on the types of SCCs and their responsibilities. My thanks go to Mel Sanders, SCC18 chair, for contributing most of the information that follows, which expands on my earlier column. [J87]

"Joint Channel Estimation and PTS to Reduce Peak-to-Average-Power Radio in OFDM Systems Without Side Information"

In this letter, we propose a novel scheme to reduce the PAPR of OFDM signals, and its key idea is that the side information of partial transmit sequence is considered as a part of channel frequency response. Therefore, the proposed scheme does not need to reserve bits for submitting side information, resulting in an increase in the data rate. Furthermore, we propose a novel pilot arrangement, in which pilot tones are independently inserted into each subblock. Simulations show that the proposed scheme with the novel pilot arrangement could offer good performances of bit error rate and PAPR reduction. [J88]

"Sharing location in online social networks"

Online social networks (OSNs) have become important media for information sharing among Internet users. In particular, several OSNs provide mechanisms to facilitate sharing of the users' location, which is gaining increased popularity due to the growth of GPS-equipped smartphones. These location-based OSNs (LSNs) bridge users' physical and social worlds, allowing users to know where their friends are and enabling location-based information access and user interactions. In this article we first introduce several LSNs and compare their location-sharing related features. A user's location, however, is sensitive and personal information that may raise significant privacy concerns. To understand real-world users' location-sharing behavior, we collected 21 months of data traces from a commercial LSN and analyzed its users' location-sharing updates. We found that the characteristics of the users' privacy protection behavior is correlated with their age, gender, mobility, and geographic region. In addition, friends tend to have similar privacy protection patterns. To the best of our knowledge, this article is the first large-scale empirical study of a modern LSN. [J89]

"Multiple Transient Faults in Combinational and Sequential Circuits: A Systematic Approach"

Transient faults in logic circuits are becoming an important reliability concern for future technology nodes. Radiation-induced faults have received significant attention in recent years, while multiple transients originating from a single radiation hit are predicted to occur more often. Furthermore, some effects, like reconvergent fanout-induced glitches, are more pronounced in the case of multiple faults. Therefore, to guide the design process and the choice of circuit optimization techniques, it is important to model multiple faults and their propagation through logic circuits, while evaluating the changes in error rates resulting from multiple simultaneous faults. In this paper, we show how output error probabilities change with increasing number of simultaneous faults and we also analyze the impact of multiple errors in state flip-flops, during the cycles following the cycle when fault(s) occurred. The results obtained using the proposed framework show that output error probability resulting from multiple-event transient or multiple-bit upsets can vary across different outputs and different circuits by several orders of magnitude. The results also show that the impact of different masking factors also varies across circuits and this information can be valuable for customizing protection techniques. [J90]

"Signal transmission with unequal error protection in relay selection networks"

A relaying technique based on single-relay selection is studied for multiple-relay networks when hierarchical modulation is employed for unequal error protection. A single-relay selection scheme achieves a higher bandwidth efficiency while maintaining the same diversity order as when all the relays are selected in a multiple-relay network. Specifically, a cooperative network with one source, Krelays, and one destination is considered in which two different protection information classes are modulated by a hierarchical 2/4-amplitude shift keying (ASK) constellation at the source. After selecting a relay to cooperate with the source, based on the instantaneous received signal-to-noise ratio, the selected relay decides to retransmit both classes by using a hierarchical 2/4-ASK constellation, or the more protection class by using a 2-ASK constellation, or remains silent. The approximated bit error rate (BER) of each information class is derived. Optimal thresholds are chosen to minimise the BER of one class while the BER of the other class satisfies a requirement. Numerical and simulation results are provided to validate the analysis. The results also show that the optimal thresholds can improve the error performance significantly. [J91]

"Design Improvement of a 245-kV Circuit Breaker With Double-Speed Mechanism Through Current Zero Analysis"

This paper presents the results of current zero measurements during short-line fault interruption tests performed on three variants of an SF6circuit breaker (CB) (245 kV, 40 kA) with a new mechanism for increasing the contact

motion speed, shortly named double-speed mechanism, in order to distinguish between double-motion systems where both contacts are moving. The application of a double-speed mechanism provides the necessary increase of contact separation speed, without a significant increase of opening energy. Besides that, it does not requires any fixed mechanical connection between the stationary and moving contacts through the nozzle. This feature has a positive impact on the CB reliability and creates the possibility of easier assembly and dismantling of the interrupter from its insulator. High-resolution measurements of near current-zero arc current and voltage were carried out during these tests. Different levels of information on the "quality of interruption," obtained from current zero measurements are presented. Direct observation of arc current and arc voltage data are analyzed. The arc conductivity very shortly (500 and 200 ns) before current zero, as an indicator of the performance of the breaker under test is discussed. All information obtained during current zero measurement is in correlation with the direct results of testing and with design improvements in successive variants of the CB. [J92]

"Privacy-Preserving Sharing of Sensitive Information"

Privacy-preserving sharing of sensitive information (PPSSI) is motivated by the increasing need for entities (organizations or individuals) that don't fully trust each other to share sensitive information. Many types of entities need to collect, analyze, and disseminate data rapidly and accurately, without exposing sensitive information to unauthorized or untrusted parties. Although statistical methods have been used to protect data for decades, they aren't foolproof and generally involve a trusted third party. Recently, the security research community has studied —and, in a few cases, deployed—techniques using secure, multiparty function evaluation, encrypted keywords, and private information retrieval. However, few practical tools and technologies provide data privacy, especially when entities have certain common goals and require (or are mandated) some sharing of sensitive information. To this end, PPSSI technology aims to enable sharing information, without exposing more than the minimum necessary to complete a common task. [J93]

"Level, Class, and Prospected Safety Performance of a Lightning Protection System for a Complex of Structures (LPCS)"

The Standard IEC 62305 provides advanced information for the design of lightning protection of structures (LPS). In determining the position of the air-termination system, two methods are generally suggested: the protective angle method and the rolling sphere method. Adopting a 3-D graphical simulation, the "rolling sphere" method allows one: to analyze the protected volume at the building roof inside of the rolling ply surface; to verify the behavior of the designed air-termination system; to evaluate the contribution of the surrounding structures in limiting the lightning current flowing in the down-conductors. This current affects the probability of dangerous sparking and the separation distance for the protection of internal installations. This paper presents this approach by a case study of a building in a complex of structures: it highlights particularly the worst cases of the lightning impact related to the designed air-termination system. [J94]

"The Dangers of Grounding Resistor Failure"

A resistance-grounded power system has a critical element that is often ignored-the neutral-grounding resistor (NGR). During a single-phase-to-ground fault, current flows from the transformer or generator winding through the faulted-phase conductor to the fault and to ground, returning to the source winding through the ground-return path and the NGR. The information presented here has shown that an open NGR is an undesirable situation. A system with an open NGR is subject to transient overvoltages, and so current sensing ground-fault protection will not indicate the presence of a ground fault. A ground fault then remains on the system and might escalate to a phase-to-phase fault. NGRs are subject to failures related to thermal overload, lightning, storms, earthquakes, wildlife, extended service life, manufacturing defects, vibration, corrosion, and improper specification or installation. A well-designed NGR monitor provides continuous protection against failures that previously rendered ground-fault protection, coordination, and annunciation systems inoperative, as well as leaving the system exposed to damaging transient overvoltages. An NGR monitor provides confidence that current-sensing ground-fault protection will operate as designed on the next ground fault. [J95]

"Energy Efficiency in Telecom Optical Networks"

Since the energy crisis and environmental protection are gaining increasing concerns in recent years, new research topics to devise technological solutions for energy conservation are being investigated in many scientific disciplines. Specifically, due to the rapid growth of energy consumption in ICT (Information and Communication Technologies), lot of attention is being devoted towards "green" ICT solutions. In this paper, we provide a comprehensive survey of the most relevant research activities for minimizing energy consumption in telecom networks, with a specific emphasis on those employing optical technologies. We investigate the energy-minimization opportunities enabled by optical technologies and classify the existing approaches over different

network domains, namely core, metro, and access networks. A section is also devoted to describe energy-efficient solutions for some of today's important applications using optical network technology, e.g., grid computing and data centers. We provide an overview of the ongoing standardization efforts in this area. This work presents a comprehensive and timely survey on a growing field of research, as it covers most aspects of energy consumption in optical telecom networks. We aim at providing a comprehensive reference for the growing base of researchers who will work on energy efficiency of telecom networks in the upcoming years. [J96]

"Performance Evaluation of Impairment-Aware Routing Under Single- and Double-Link Failures"

This work evaluates the performance of an impairment-aware routing (IAR) scheme in the presence of single- and dual-link failures. Network resilience is provided through a shared backup path protection scheme, enhanced with a reinforced sharing mechanism. The results indicate that the IAR scheme provides significantly lower connection blocking compared with traditional minimum-hop routing because physical impairments have a significant contribution to the overall network blocking probability. Dual-link failures are also considered, and the performance of a network designed to be resilient to single-link failures is evaluated. Simulation results show low connection loss rates due to dual failures that can be further improved using a restoration mechanism activated on the occurrence of dual failures. [J97]

"RAIM with Optimal Integrity and Continuity Allocations Under Multiple Failures"

Among the receiver autonomous integrity monitoring (RAIM) algorithms treating multiple failures, multiple hypothesis solution separation algorithms (MHSS)—a type of solution separation algorithm—offer several advantages: First, the link between threat model, upper bound on the position error—the protection level and probability of hazardously misleading information is an easy and straightforward one; second, the calculation of the protection level does not involve complex steps. One of the critical steps in this algorithm is the allocation of the integrity and continuity budgets among the failure modes, as it determines the overall performance of the algorithm. After describing the baseline MHSS approach, we present an algorithm that simultaneously allocates the integrity and continuity budget among the failure modes to obtain the minimum protection level per satellite geometry. Then, we show how slope-based RAIM and solution separation RAIM are related through a little-known formula, which both unifies and highlights the differences between the two approaches. Finally, we apply the algorithm to evaluate the performance of RAIM for vertical guidance for a dual constellation, and find that even with a very large prior probability of satellite failure, vertical guidance can be achieved worldwide with high availability. [J98]

"An Adaptive Multiagent Approach to Protection Relay Coordination With Distributed Generators in Industrial Power Distribution System"

This paper presents new explorations into the use of agent technology applied to the protection coordination of power systems. The impact of distributed generators on protection coordination is first discussed. Then, a coordination multiagent system is proposed with the functions of the agents described. In the proposed system, communication will play an important role to provide more information for the relay coordination besides the relay settings. Communication simulation has been carried out on the Java Agent Development Framework platform. The information communication process shows that adaptive coordination can be achieved. [J99]

"Cloud Computing in Developing Economies"

The developing world must exploit the opportunities afforded by cloud computing while minimizing the associated risks to allow access to advanced IT infrastructure, data centers, and applications and protect sensitive information. [J100]

"Experimental Performance of Shared Path Protection With Flooded Versus Collected Sharing Resource Information in GMPLS WSON Networks"

In generalized multiprotocol label switching (GMPLS)-enabled wavelength-switched optical networks (WSONs), shared path protection (SPP) attains 100% survivability with an acceptable recovery time, for lightpaths affected by a single-link failure. This is achieved by sharing backup resources. Nevertheless, neither the standard OSPF-TE nor the RSVP-TE protocols support the respective flooding/collection of shareable resource information for SPP purposes. This prevents the source node from computing backup paths exploiting the SPP advantages, and the destination node from performing optimal wavelength assignment (WA) favoring the reuse of shareable resources. In this paper, we experimentally evaluate, in the GMPLS control plane of the ADRENALINE testbed, the performance improvements when shareable resource information is either flooded (by enhanced OSPF-TE) and/or collected (by enhanced RSVP-TE), under the wavelength continuity constraint. Additionally, we propose

efficient SPP path computation and WA algorithms, considering three information dissemination strategies: aggregated unreserved bandwidth, aggregated shared bandwidth, and wavelength-channel granularity. [J101]

"McWiLL-A New Mobile Broadband Access Technology for Supporting Both Voice and Packet Services"

As an evolution from Synchronous Code Division Multiple Access (SCDMA), McWiLL (Multi-Carrier Wireless Information Local Loop) mobile broadband access technology was proposed to work with Next Generation Networks (NGNs) to offer various content-rich services. Several core state-of-the-art technologies used in McWiLL mobile broadband access system are introduced in this paper, such as smart antennas, CS-OFDMA (Code Spreading Orthogonal Frequency Division Multiple Access), adaptive modulation, dynamic channel allocation, make-before-break handoff, and fraud protection, etc. These key techniques allow McWiLL to support a large coverage, high spectrum efficiency (up to 3 bit/s/Hz), a homogeneous service quality between high and low rate traffics, low cost terminals, and high mobility applications. McWiLL was designed in particular to suit for its applications in hostile environments due to its superb interference cancellation capability, special frame structure design, and dynamic channel assignment scheme. [J102]

"Location privacy in urban sensing networks: research challenges and directions [JSecurity and Privacy in Emerging Wireless Networks]"

During the last few years there has been an increasing number of people-centric sensing projects. These combine location information with sensors available on mobile phones, giving birth to a different dimension in sensing our environment and providing us with new opportunities to create collective intelligence systems to address urban-scale problems such as air pollution, noise, and traffic. However, as people are directly involved in the collection process, they often inadvertently reveal information about themselves, raising new and important privacy concerns. While standard privacy enhancing technologies exist, they do not fully cover the many peculiarities of these new pervasive applications. The ubiquitous nature of the communication and the storage of location traces compose a complex set of threats on privacy, which we overview in this article. Then we go through the latest advances in security and privacy protection strategies, and discuss how they fit with this new paradigm of people-centric sensing applications. We hope this work will better highlight the need for privacy in urban sensing applications and spawn further research in this area. [J103]

"Resilience to Degree-Dependent and Cascading Node Failures in Random Geometric Networks"

This paper studies the problem of resilience to node failures in large-scale networks modelled by random geometric graphs. Adopting a percolation-based viewpoint, the paper investigates the ability of the network to maintain global communication in the face of dependent node failures. Degree-dependent site percolation processes on random geometric graphs are examined, and the first known analytical conditions are obtained for the existence and non-existence, respectively, of a large connected component of operational network nodes after degree-dependent node failures. In electrical power networks or wireless communication and computing networks, cascading failure from power blackouts or virus epidemics may result from a small number of initial node failures triggering global failure events affecting the whole network. With the use of a simple but descriptive model, it is shown that the cascading failure problem is equivalent to a degree-dependent percolation process. The first analytical conditions are obtained for the occurrence and non-occurrence of cascading failures, respectively, in large-scale networks with geometric constraints. [J104]

"Digital product transaction mechanism for electronic auction environment"

The rapid development in electronic commerce and information technology drives the traditional physical product trading evolved to digital product trading. With the effect of the multi-agents system in the Internet environment and the promotions of Government, digital product industry grows fast. The authors proposed a digital product transaction mechanism for electronic auction in the multi-agents system environment. The research introduced a convenient platform to protect the privacies of both buyers and sellers, and track digital product further in an electronic auction environment. In addition, by using simple cryptography techniques supplemented with encryption, the authors ensure the security of information transactions, thereby providing a mechanism of safe and fair digital product electronic auction. [J105]

"Anonymity and security for autonomous mobile agents"

The mobile agent security against malicious hosts is one of the most important subjects in mobile agent technology. An extended requirement for an agent security in different applications is to provide it with anonymity property in such a way that the agent can travel in the network without exposing its owner identity and its

itinerary. For this purpose, an agent anonymity protocol is proposed to maintain the anonymity of the agent owner and the agent itinerary. The introduced anonymous agent is also applied to disarm the host against the agent instead of using an armed agent, that is, an agent equipped with protection mechanisms. The analytical discussion demonstrated that this protocol preserves the autonomy of the agent in choosing the migration path and is also resistant against known traffic analysis attacks in mobile agent systems with plausible assumption. Moreover, it is feasible and adjustable regarding the required level of anonymity. [J106]

"Robust Transmission and Interference Management For Femtocells with Unreliable Network Access"

A cellular system where macrocells are overlaid with femtocells is studied. Each femtocell is served by a home base station (HBS) that is connected to the macrocell base station (BS) via an unreliable network access link, such as DSL followed by the Internet. A scenario with a single macrocell and a single femtocell is considered first, and is then extended to include multiple macrocells and femtocells, both with standard single-cell processing and with multicell processing (or network MIMO). Two main issues are addressed for the uplink channel: (i) Interference management between femto and macrocells; (ii) Robustness to uncertainties on the quality of the femtocell (HBSto-BS) access link. The problem is formulated in information-theoretic terms, and inner and outer bounds are derived to achievable per-cell sum-rates for outdoor and home users. Expected sum-rates with respect to the distribution of the femtocells access link states are studied as well. Overall, the analysis lends evidence to the performance advantages of sophisticated interference management techniques, based on joint decoding and relaying, and of robust coding strategies via the broadcast coding approach (i.e., unequal error protection). [J107]

"Covert channel resistant information leakage protection using a multi-agent architecture"

Covert channel attacks utilise shared resources to indirectly transmit sensitive information to unauthorised parties. Current operating systems (e.g. SELinux) rely on tagging the filesystem with security labels and enforcing security policies at the time of access to a file or resource. However, such mechanisms do not provide strong protection against information laundering via covert channels. Colored Linux, an extension to SELinux, utilises watermarking algorithms to `colour` the contents of each file with their respective security classification, or context, to enhance resistance to information laundering attacks. In this study, the authors propose a mobile agent-based approach to automate the process of detecting and colouring receptive hosts` filesystems and monitoring the coloured filesystem for instances of potential information leakage. Implementation details and execution results are included to illustrate the merits of the proposed approach. The authors have also evaluated the performance of their agent-based system over a single host as well as a local network of machines. Finally, using formal method techniques, the authors have proved correctness properties about the agent-based approach and identified and corrected a flaw in their initial implementation. [J108]

"A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation"

The increasing popularity of the internet means that digital multimedia are transmitted more rapidly and easily. And people are very aware for media ownership. However, digital watermarking is an efficient and promising means to protect intellectual properties. Based on the intellectual property attention in the information era, how to protect the personal ownership is extremely important and a necessary scheme. In this paper, we propose an effective video watermarking method based on a pseudo-3-D discrete cosine transform (DCT) and quantization index modulation (QIM) against several attacks. The watermark is mainly inserted into the uncompressed domain by adjusting the correlation between DCT coefficients of the selected blocks, and the watermark extraction is blind. This approach consists of a pseudo-3-D DCT, watermark embedding, and extraction. A pseudo-3-D DCT, which is taken DCT transformation twice, will be first utilized to calculate the embedding factor and to obtain the useful messages. Using the QIM, we embed the watermark into the quantization regions from the successive raw frames in the uncompressed domain and record the relative information to create a secret embedding key. This secret embedding key will further apply to extraction. Experimental results demonstrate that the proposed method can survive filtering, compressions, luminance change, and noise attacks with a good invisibility and robustness. [J109]

"PSO and ANN-based fault classification for protective relaying"

Fault classification in electric power system is vital for secure operation of power systems. It has to be accurate to facilitate quick repair of the system, improve system availability and reduce operating costs due to mal-operation of relay. Artificial neural networks (ANNs) can be an effective technique to help to predict the fault, when it is provided with characteristics of fault currents and the corresponding past decisions as outputs. This paper describes the use of particle swarm optimisation (PSO) for an effective training of ANN and the application

of wavelet transforms for predicting the type of fault. Through wavelet analysis, faults are decomposed into a series of wavelet components, each of which is a time-domain signal that covers a specific octave frequency band. The parameters selected for fault classification are the detailed coefficients of all the phase current signals, measured at the sending end of a transmission line. The information is then fed into ANN for classifying the faults. The proposed PSO-based multi-layer perceptron neural network gives 99.91% fault classification accuracy. Moreover, it is capable of producing fast and more accurate results compared with the back-propagation ANN. Extensive simulation studies were carried out and a set of results taken from the simulation studies are presented in this paper. The proposed technique when combined with a wide-area monitoring system would be an effective tool for detecting and identifying the faults in any part of the system. [J110]

"Region Duplication Detection Using Image Feature Matching"

Region duplication is a simple and effective operation to create digital image forgeries, where a continuous portion of pixels in an image, after possible geometrical and illumination adjustments, are copied and pasted to a different location in the same image. Most existing region duplication detection methods are based on directly matching blocks of image pixels or transform coefficients, and are not effective when the duplicated regions have geometrical or illumination distortions. In this work, we describe a new region duplication detection method that is robust to distortions of the duplicated regions. Our method starts by estimating the transform between matched scale invariant feature transform (SIFT) keypoints, which are insensitive to geometrical and illumination distortions, and then finds all pixels within the duplicated regions after discounting the estimated transforms. The proposed method shows effective detection on an automatically synthesized forgery image database with duplicated and distorted regions. We further demonstrate its practical performance with several challenging forgery images created with state-of-the-art tools. [J111]

"Data-Centric Privacy Protocol for Intensive Care Grids"

Modern e-Health systems require advanced computing and storage capabilities, leading to the adoption of technologies like the grid and giving birth to novel health grid systems. In particular, intensive care medicine uses this paradigm when facing a high flow of data coming from intensive care unit's (ICU) inpatients just like demonstrated by the ICGrid system prototyped by the University of Cyprus. Unfortunately, moving an ICU patient's data from the traditionally isolated hospital's computing facilities to data grids via public networks (i.e., the Internet) makes it imperative to establish an integral and standardized security solution to avoid common attacks on the data and metadata being managed. Particular emphasis must be put on the patient's personal data, the protection of which is required by legislations in many countries of the European Union and the world in general. In this paper, we extend our previous research with the following contributions: 1) a mandatory access control model to protect patient's metadata; 2) a major security revision to our previously proposed privacy protocol by contributing with a "quality of security" quantitative metric to improve fragmented data's assurance; and finally, 3) a set of early results to demonstrate that our protocol not only improves a patient personal data's security and privacy but also achieves a performance comparable with existing approaches. [J112]

"Automated Control System Security"

Automated control systems (ACSs) lie at the heart of industrial and infrastructure systems and, as such, are one of the most critical parts of critical infrastructures. Yet the information security world has largely ignored these systems, and most information security folks seem to think that the protective processes, measures, and mechanisms that apply to general-purpose enterprise computers also apply to ACSs. At the same time, most control systems engineers know almost nothing about information protection and don't recognize even the potential for the sorts of things that information security professionals consider standard. This mismatch must be addressed, or we'll be paying the price for it for at least one generation. [J113]

"Data Tagging for New Information Governance Models"

The ubiquitous collection, use, and flow of data challenge existing frameworks for data protection and management. Organizations collect and derive data from myriad sources and use it for various purposes, so that the rules that apply to their data holdings vary. The authors describe data governance in this complex and dynamic environment, where the rules and obligations that govern how organizations use and protect information attach to the data and must be met wherever or by whomever collects, processes, or stores it. They suggest data tagging to facilitate such an approach. [J114]

"Kernel Service Protection for Client Security"

Authentication within the X86 CPU system management mode has significant benefits for system security. The

author's mechanism lets system firmware access cipher information from a software application image to check code integrity for security-sensitive code. [J115]

"Proliferation and Detection of Blog Spam"

The ease of posting comments and links in blogs has attracted spammers as an alternative venue to conventional email. An experimental study investigates the nature and prevalence of blog spam. Using Defensio logs, the authors collected and analyzed more than one million blog comments during the last two weeks of June 2009. They used a support vector machine (SVM) classifier combined with heuristics to identify spam posters' IP addresses, autonomous system numbers (ASN), and IP blocks. Experimental results show that more than 75 percent of blog comments during the reporting period are spam. In addition, the results show that blog spammers likely operate from a few colocation facilities. [J116]

"Optimal power allocation for OFDM-based cognitive radio with new primary transmission protection criteria"

This paper considers a spectrum underlay network, where an OFDM-based cognitive radio (CR) system is allowed to share the subcarriers of an OFDMA-based primary system for simultaneous transmission. Instead of using the conventional interference power constraint (IPC) to protect the primary users (PUs) in the primary system, a new criterion referred to as rate loss constraint (RLC), in the form of an upper bound on the maximum rate loss of each PU due to the CR transmission, is proposed for primary transmission protection. Assuming the channel state information (CSI) of the PU link, the CR link, and their mutual interference links is available to the CR, the optimal power allocation strategy to maximize the achievable rate of the CR system is derived under RLC together with CRïs transmit power constraint. It is shown that the CR system can achieve a significant rate gain under RLC as compared to IPC. Furthermore, the relationship between RLC and IPC is investigated, and it is shown that the rate gain is obtained by exploiting the additional CSI of the PU link. A more general case referred to as hybrid protection to PUs is then studied, by taking into account that some PU linksï CSI is not available at CR. [J117]

"Online Anonymity Protection in Computer-Mediated Communication"

In any situation where a set of personal attributes are revealed, there is a chance that revealed data can be linked back to its owner. Examples of such situations are publishing user profile micro-data or information about social ties, sharing profile information on social networking sites, or revealing personal information in computer-mediated communication (CMC). Measuring user anonymity is the first step to ensuring that the identity of the owner of revealed information cannot be inferred. Most current measures of anonymity ignore important factors such as the probabilistic nature of identity inference, the inferrer's outside knowledge, and the correlation between user attributes. Furthermore, in the social computing domain, variations in personal information and various levels of information exchange among users make the problem more complicated. We present an information-entropy-based realistic estimation of the user anonymity level to deal with these issues in social computing in an effort to help predict the identity inference risks. We then address implementation issues of online protection by proposing complexity reduction methods that take advantage of basic information entropy properties. Our analysis and delay estimation based on experimental data show that our methods are viable, effective, and efficient in facilitating privacy in social computing and synchronous CMCs. [J118]

"An Intelligent Secure and Privacy-Preserving Parking Scheme Through Vehicular Communications"

There are always frustrations for drivers in finding parking spaces and being protected from auto theft. In this paper, to minimize the drivers' hassle and inconvenience, we propose a new intelligent secure privacy-preserving parking scheme through vehicular communications. The proposed scheme is characterized by employing parking lot RSUs to surveil and manage the whole parking lot and is enabled by communication between vehicles and the RSUs. Once vehicles that are equipped with wireless communication devices, which are also known as onboard units, enter the parking lot, the RSUs communicate with them and provide the drivers with real-time parking navigation service, secure intelligent antitheft protection, and friendly parking information dissemination. In addition, the drivers' privacy is not violated. Performance analysis through extensive simulations demonstrates the efficiency and practicality of the proposed scheme. [J119]

"Classification of Grassland Types by MODIS Time-Series Images in Tibet, China"

Tibet is one of the five largest pasturing regions of China. Grassland classification is significant for its utilization and protection, but few correlative studies have been done in Tibet due to its rugged natural conditions, which

make it difficult and time-consuming to conduct extensive field measurements. The remote-sensing technique is helpful for grassland classification in such regions. In this study, high temporal resolution of a moderate resolution imaging spectroradiometer (MODIS) is used to construct temporal profiles of enhanced vegetation index (EVI) during the grass growth period in Tibet. By dividing the large study area into individual regions based on altitude and latitude, we classified the grasslands of Tibet into six types-meadow steppe, typical steppe, desert steppe, alpine meadow steppe, alpine typical steppe, and shrub herbosa. Based on the 1:500 000 scale maps of China's grassland resources, the validation process indicates an overall accuracy of 68.02 %, and a Kappa coefficient of 0.52. Land managers are provided with maps and area values of each grassland type in Tibet in 2005. In addition, regional average EVI reflect the relative biomass of each types of the grassland, which will provide evidences for coordinating plans for grassland developing. MODIS_EVI provides a simple and rapid method to classify the grassland in regions that are hard to reach, which offers an effective means of investigating biological resources on a large scale. [J120]

"A Perceptually Tuned Watermarking Scheme for Color Images"

Transparency and robustness are two conflicting requirements demanded by digital image watermarking for copyright protection and many other purposes. A feasible way to simultaneously satisfy the two conflicting requirements is to embed high-strength watermark signals in the host signals that can accommodate the distortion due to watermark insertion as part of perceptual redundancy. The search of distortion-tolerable host signals for watermark insertion and the determination of watermark strength are, hence, crucial to the realization of a transparent yet robust watermark. This paper presents a color image watermarking scheme that hides watermark signals in most distortion-tolerable signals within three color channels of the host image without resulting in perceivable distortion. The distortion-tolerable host signals or the signals that possess high perceptual redundancy are sought in the wavelet domain for watermark insertion. A visual model based upon the CIEDE2000 color difference equation is used to measure the perceptual redundancy inherent in each wavelet coefficient of the host image. By means of quantization index modulation, binary watermark signals are embedded in qualified wavelet coefficients. To reinforce the robustness, the watermark signals are repeated and permuted before embedding, and restored by the majority-vote decision making process in watermark extraction. Original images are not required in watermark extraction. Only a small amount of information including locations of qualified coefficients and the data associated with coefficient quantization is needed for watermark extraction. Experimental results show that the embedded watermark is transparent and quite robust in face of various attacks such as cropping, low-pass filtering, scaling, media filtering, white-noise addition as well as the JPEG and JPEG2000 coding at high compression ratios. [J121]

"Electro-Thermo-Mechanical Characterizations of Various Wire Bonding Interconnects Illuminated by an Electromagnetic Pulse"

A comprehensive electro-thermo-mechanical transient investigation is carried out to characterize time-dependent thermal and mechanical responses of metal wire bonding interconnects, as they suffer from the impact of an electromagnetic pulse (EMP) with different current or voltage waveforms. In our mathematical implementation, a hybrid time-domain finite element method is applied to simulate mutual interactions among electrical, thermal, and mechanical fields, with all nonlinearities of temperature-dependent electrical conductivities, thermal conductivities, thermal expansion coefficients, and even the Young's modulus of materials being treated appropriately. The developed algorithm is partially validated by computing transient temperature and thermal stress of other interconnects with good agreement with reference results. Parametric studies are performed to show the effects of EMP waveform parameters, geometrical and physical parameters of various wire bonding interconnects on their transient thermal and mechanical responses, thus providing basic information for their electromagnetic protection so as to suppress the impact of an intentional EMP. [J122]

"Guest Editorial Special Section on Smart Wearable Devices for Human Health and Protection"

The 12 papers in this special section are original and relevant contributions in the area of smart wearable devices (SWDs) applied to the health and civil protection domain. [J123]

"A Wavelet-PCA-Based Fingerprinting Scheme for Peer-to-Peer Video File Sharing"

In order to utilize peer-to-peer (P2P) networks in legal content distribution to benefit the legal content providers, copyright protection needs to be enhanced. In this paper, a fingerprint generation and embedding method is proposed for complex P2P file sharing networks. In this method, wavelet and principal component analysis (PCA) techniques are used for fingerprint generation. First, the wavelet technique obtains a low-frequency representation of the test image (or source file, which is assumed to be one I frame of a video with a DVD quality) and PCA finds the features of the representation. Then, a set of fingerprint matrices can be created

based on a proposed algorithm. Finally, each matrix combines with the low-frequency representative to become a unique fingerprinted matrix. The fingerprinted matrix is not only much smaller than the original image in size but also contains the most important information. Without this information, the quality of the reconstructed image will be very poor. Thus, the fingerprinted file is more suitable for distribution in P2P networks, because, in the distribution stage, the uniquely fingerprinted matrix will only be dispensed by the source host and leave the rest for P2P networks to handle. On the other hand, among other frames of the same video which are not decomposed, some will be embedded with sharable fingerprints. The relationship between unique fingerprint and sharable fingerprint and the purpose of using it will be discussed in the paper. Our result indicates that the proposed fingerprint has shown strong robustness against common attacks such as Gaussian noise, median filter, and lossy compression. [J124]

"Source-channel rate optimization for progressive image transmission over block fading relay channels [JTransactions Papers]"

In this paper, we are concerned with the design and analysis of joint source-channel coding schemes for block fading channels with relay-assisted distributed spatial diversity. Assuming a progressive image coder with a constraint on the transmission bandwidth, we formulate a joint source-channel rate allocation scheme that maximizes the expected source throughput. Specifically, using Gaussian as well as BPSK inputs on flat Rayleigh fading channels, we lower bound the average packet error rate by the corresponding mutual information outage probability, and derive the average throughput expression as a function of channel code rates as well as channel SNR for both a frequency-division multiplexing-based baseline system without relaying, and a half-duplex relay system with a decode-and- forward protocol. At high signal-to-noise ratio (SNR), for the systems considered in this paper, we show that our rate optimization problem is a convex function of the channel code rates, and we show that a known recursive algorithm can be used to predict the performance of both systems. [J125]

"A Rule-Based Trust Negotiation System"

Open distributed environments, such as the World Wide Web, facilitate information sharing but provide limited support to the protection of sensitive information and resources. Trust negotiation (TN) frameworks have been proposed as a better solution for open environments, in which parties may get in touch and interact without being previously known to each other. In this paper, we illustrate Protune, a rule-based TN system. By describing Protune, we will illustrate the advantages that arise from an advanced rule-based approach in terms of deployment efforts, user friendliness, communication efficiency, and interoperability. The generality and technological feasibility of Protune's approach are assessed through an extensive analysis and experimental evaluations. [J126]

"Evaluation of Power Constant Dual-Rail Logics Countermeasures against DPA with Design Time Security Metrics"

Cryptographic circuits are nowadays subject to attacks that no longer focus on the algorithm but rather on its physical implementation. Attacks exploiting information leaked by the hardware implementation are called side-channel attacks (SCAs). Among these attacks, the differential power analysis (DPA) established by Paul Kocher et al. in 1998 represents a serious threat for CMOS VLSI implementations. Different countermeasures that aim at reducing the information leaked by the power consumption have been published. Some of these countermeasures use sophisticated back-end-level constraints to increase their strength. As suggested by some preliminary works (e.g., by Li from Cambridge University), the prediction of the actual security level of such countermeasures remains an open research area. This paper tackles this issue on the example of the AES SubBytes primitive. Thirteen implementations of SubBytes, in unprotected, WDDL, and SecLib logic styles with various back-end-level arrangements are studied. Based on simulation and experimental results, we observe that static evaluations on extracted netlists are not relevant to classify variants of a countermeasure. Instead, we conclude that the fine-grained timing behavior is the main reason for security weaknesses. In this respect, we prove that SecLib, immune to early-evaluation problems, is much more resistant against DPA than WDDL. [J127]

"Joint Decoding of Unequally Protected JPEG2000 Bitstreams and Reed-Solomon Codes"

In this paper we present joint decoding of JPEG2000 bitstreams and Reed-Solomon codes in the context of unequal loss protection. Using error resilience features of JPEG2000 bitstreams, the joint decoder helps to restore the erased symbols when the Reed-Solomon decoder fails to retrieve them on its own. However, the joint decoding process might become time-consuming due to a search through the set of possible erased symbols. We propose the use of smaller codeblocks and transmission of a relatively small amount of side information with high reliability as two approaches to accelerate the joint decoding process. The accelerated joint decoder can deliver essentially the same quality enhancement as the nonaccelerated one, while operating

several times faster. [J128]

"Improved Fault-Location System for Railway Distribution System Using Superimposed Signal"

The railway distribution system is a neutral noneffectively grounded medium-voltage network. An advanced fault-location system for this distribution network, called the railway distribution network fault location system, is proposed in this paper. This fault-location system is based on tracing the superimposed signal and the work principle, simulation results, and field tests of the location system are presented. It is able to identify the fault location in a fast and accurate way. Compared with other conventional superimposed signal-based schemes, the system's performance is improved by employing the inject and fault-current detect sensor (IFCDS) to trace the fault signal and wireless to transmit detect information. The IFCDS, which permanently hangs on feeders, is based on the wireless sensor networks technology, so it can network automatically in a certain range, and improve the flexibility of the communication subsystem. Through analyzing the uploaded information by the fault-location computer in the substation, the fault point can be located. Issues of superimposed signals, such as optimal frequency choice, impact of tapped load, fault distance, and fault resistance, and so on are of concern. Through simulation in PSCAD/EMTDC, these issues are fully discussed. At last, the tests in the field show that the system has simple principle, high reliability, fast location speed (usually less than 15 min), and high accuracy (location error is less than 0.5 km). [J129]

"Correcting Limited-Magnitude Errors in the Rank-Modulation Scheme"

We study error-correcting codes for permutations under the infinity norm, motivated by a novel storage scheme for flash memories called rank modulation. In this scheme, a set of nflash cells are combined to create a single virtual multilevel cell. Information is stored in the permutation induced by the cell charge levels. Spike errors, which are characterized by a limited-magnitude change in cell charge levels, correspond to a low-distance change under the infinity norm. We define codes protecting against spike errors, called limited-magnitude rank-modulation codes (LMRM codes), and present several constructions for these codes, some resulting in optimal codes. These codes admit simple recursive, and sometimes direct, encoding and decoding procedures. We also provide lower and upper bounds on the maximal size of LMRM codes both in the general case, and in the case where the codes form a subgroup of the symmetric group. In the asymptotic analysis, the codes we construct outperform the Gilbert-Varshamov-like bound estimate. [J130]

"Comparison of Automatic DSM Generation Modules by Processing IKONOS Stereo Data of an Urban Area"

This study deals with the evaluation of four different image-processing software modules for the generation of digital surface models from very high-resolution stereo satellite data. The analysis was done in an urban area due to the growing interest in 3-D information over built-up areas. Depending on the different geometric model approaches used by the different software packages, shifts between 3.06-3.27 m between the digital surface models (DSMs) and the reference DSM were measured. The vertical RMSE of the four tested software packages range between 2.96-14.01 m. However, the visual evaluation resulted in a different ranking and does not confirm the quantitative results entirely. The results show that, depending on the building type to be extracted, the choice of software package may vary. The challenges of automatic DSM extraction in urban areas and the performance of current software package modules to address them are discussed. Potential improvements for automatic DSM extraction in urban areas are identified. [J131]

"A Field Study of Lightning Surges Propagating Into Residences"

In the highly information-based society of today, lightning damage to home electric appliances, such as personal computers and facsimile machines is having a greater impact, indicating a growing public interest in countermeasures for lightning. However, many things remain unknown about lightning surges that propagate into residences. The Tokyo Electric Power Company had observed the patterns of intrusion of lightning surges into residences using lightning surge waveform detectors installed at ordinary residences and obtained observation data on 18 lightning strokes between 2003 and 2006. These observation results can be used to examine the patterns of propagation of lightning surges into residences. In some observation cases of lightning strokes to the ground, lightning surge currents were estimated to flow from the ground into residences. These valuable data will be useful for elucidating the lightning surge propagation in the low-voltage distribution system including residences. [J132]

"A Transfer-Function-Based Thermal Model Reduction Study for Induction Machine Thermal Overload Protective Relays"

High-order induction machine thermal models have been widely studied for the analysis of the thermal behavior of induction machines. However, the real-time implementation of such models for the online thermal protection of induction machines is very difficult due to the lack of accurate information on the machines. This paper proposes a novel simplified thermal model of induction machines for thermal overload relays. Instead of using a lumped thermal network, a transfer-function-based approach is proposed for reducing the order of induction machine thermal models. The proposed thermal model requires significantly fewer thermal parameters for the accurate modeling of the thermal behavior of the machine. The proposed thermal model is validated via experimental results on a 7.5-hp open-drip-proof induction machine under various load conditions. The major features of the proposed thermal model are the following: 1) high accuracy of the stator winding temperature estimation, with a root-mean-square error within 3°C; 2) low computational requirement, which reduces the cost of thermal overload relays; and 3) easy implementation since only current sensors are required. [J133]

"Impact of Available Fault Current Variations on Arc-Flash Calculations"

Prior to the arrival of the arc-flash hazard analysis and the incident energy calculations, it was common practice to perform short-circuit studies assuming an infinite source on the primary of the service transformer. With the main goal of a short-circuit study being to compare the maximum calculated short-circuit current to the short-circuit rating of protective devices, using an infinite source resulted in the most conservative short-circuit current. However, since the amount of energy available in an arc-flash incident is not only dependent on the available short-circuit current but also on the clearing time of the protective device, the assumption of an infinite source on the transformer primary will not guarantee the most conservative results for the incident energy calculations downstream of the transformer. This paper examines the effect of the utility available fault current on the incident energy calculations and proposes a new method to calculate the conservative arc-flash results in the event that the actual utility fault information is not available. [J134]

"Free/Open Services"

A novel concept of free/open services adopts the principles of the free/ open source software approach and adapts them for service-oriented computing to enhance the widespread use of services. [J135]

"Simulation and Measurements of Stray Minority Carrier Protection Structures in CMOS Image Sensors"

Recently, the rapid growth of CMOS technology has made it possible to integrate more periphery circuits into a CMOS image sensor. Although these periphery circuits improve image quality, they also lead to the generation of more stray minority carriers. Because the number of stray minority carriers is proportional to the frequency, the affected region increases with increasing operating frequency. Placing an appropriate absorber between the periphery circuits and the pixel has traditionally been accepted as the best solution for this issue. Four protection tactics were simulated in software and verified in a fabricated CMOS image sensor. The imager was fabricated using TSMC 1-poly 6-metal 0.18-μm process technology. On this chip, ten noise sources outside the pixel array were used to verify the effectiveness of the protection tactics in off-array tests, whereas in-pixel noise sources were used in in-pixel tests. To quantify the influence of stray minority carriers in the off-array test, the maximum depth of an affected region (DAR) was measured in a processed binary image. The off-array experimental results revealed that the DAR increased with either an increased operating frequency or a decreased separation between the noise source and the pixel array. The DAR of the affected pixels can be eliminated up to 48.1% and 23.8% by using the N-well and N-diffusion guard rings, respectively. The in-pixel experimental results have shown that the N-diffusion digital pixel implementation reduced the noise by 63.2% while only increasing the area by 10.68%. Detailed information about the effectiveness of different protection tactics in an imager design was collected in this paper. This paper can potentially provide a reference to help imager designers choose an appropriate protection tactic. [J136]

"Web-Application Security: From Reactive to Proactive"

Here's a sobering thought for all managers responsible for Web applications: Without proactive consideration for an application's security, attackers can bypass nearly all lower-layer security controls simply by using the application in a way its developers didn't envision. Learn how to address vulnerabilities proactively and early on to avoid the devastating consequences of a successful attack. [J137]

"CITA03-Protection of Personal Information in User-centric Converged Service Platforms"

The so-called User-Generated Services (UGS) provide users with the means to create and share their own advanced services that better fit their needs or those of their communities. Platforms supporting UGS for non-technically skilled users are becoming popular, both in the Internet and the Telecommunications domains. They

provide creators with the means to include consumers' personal data or contextual information in order to generate attractive value-added services and also to improve the user-experience. However, the use and release of personal identifiable information poses several privacy and data protection concerns. In this paper we analyze the foreseeable problems and propose a solution for the protection of personal information on a UGS platform. [J138]

"Probabilistic Resource Allocation for Opportunistic Spectrum Access"

Opportunistic spectrum access (OSA) in cognitive radio (CR) networks significantly improves spectrum efficiency by allowing secondary usage of licensed spectrum. In this paper, we propose a probabilistic resource allocation approach to further exploit the flexibility of OSA. Based on the probabilities of channel availability obtained from spectrum sensing, the proposed approach optimizes channel and power allocation in a multi-channel environment. The given algorithm maximizes the overall utility of a CR network and ensures sufficient protection of licensed users from unacceptable interference, which also supports diverse quality-of-service requirements and enables a distributed implementation in multi-user networks. Both analytical and simulation results demonstrate the effectiveness of this approach as well as its advantage over conventional approaches that rely upon the hard decisions on channel availability. [J139]

"Echonet: A Home Network Standard"

Echonet is a de jure home network standard ratified by the IEC and the ISO for control and monitor sensors, household appliances, and equipment. Its small footprint offers many unique features such as media-independent control systems, interoperability in a multiple vendor environment, compatibility with long-term ecosystem construction, and secure communication to protect personal information. [J140]

"GMPLS-based Multidomain Restoration: Analysis, Strategies, Policies and Experimental Assessment"

A connection spanning, for example, several countries crosses multiple optical backbone networks, each one controlled by different administrators or operators. In this context, the interworking of these networks is thus necessary to set up end-to-end optical connections. A key issue when delivering such optical services is the use of efficient and fast restoration strategies to recover a connection disruption. To this end, there are several issues and policies that a network operator should address, such as interdomain failure information exchange and the point of repair (PoR) placement problem. Upon a failure's occurrence, exchanging interdomain failure information results is essential to attain both an efficient use of the network resources (i.e., wavelength channels) and a fast restoration time. In this regard, within the GMPLS (Generalized Multi-Protocol Label Switching) framework, interdomain information exchange remains unstandardized. Three network operator policies are proposed to yield different restoration mechanisms according to different interdomain failure exchanges. Additionally, three PoR strategies are pointed out and are qualitatively compared. Finally, selected policies and restoration strategies are experimentally validated and compared in terms of the restoration time. Experiments have been carried out over a multidomain optical network infrastructure connecting the GMPLS-based control planes of the UPC CARISMA and the CTTC ADRENALINE test beds. [J141]

"Comparison of Multiclass SVM Classification Methods to Use in a Supportive System for Distance Relay Coordination"

This paper aims at evaluating the methods of multiclass support vector machines(SVMs) for effective use in distance relay coordination. Also, it describes a strategy of supportive systems to aid the conventional protection philosophy in combating situations where protection systems have maloperated and/or information is missing and provide selective and secure coordinations. SVMs have considerable potential as zone classifiers of distance relay coordination. This typically requires a multiclass SVM classifier to effectively analyze/build the underlying concept between reach of different zones and the apparent impedance trajectory during fault. Several methods have been proposed for multiclass classification where typically several binary SVM classifiers are combined together. Some authors have extended binary SVM classification to one-step single optimization operation considering all classes at once. In this paper, one-step multiclass classification, one-against-all, and one-against-one multiclass methods are compared for their performance with respect to accuracy, number of iterations, number of support vectors, training, and testing time. The performance analysis of these three methods is presented on three data sets belonging to training and testing patterns of three supportive systems for a region and part of a network, which is an equivalent 526-bus system of the practical Indian Western grid. [J142]

"Fault-Location System for Multiterminal Transmission Lines"

This research presents the development and implementation in a computational routine of algorithms for fault location in multiterminal transmission lines. These algorithms are part of a fault-location system, which is capable of correctly identifying the fault point based on voltage and current phasor quantities, calculated by using measurements of voltage and current signals from intelligent electronic devices, located on the transmission-line terminals. The algorithms have access to the electrical parameters of the transmission lines and to information about the transformers loading and their connection type. This paper also presents the development of phase component models for the power system elements used by the fault-location algorithms. [J143]

"Robust Regression and Lasso"

Lasso, or l1regularized least squares, has been explored extensively for its remarkable sparsity properties. In this paper it is shown that the solution to Lasso, in addition to its sparsity, has robustness properties: it is the solution to a robust optimization problem. This has two important consequences. First, robustness provides a connection of the regularizer to a physical property, namely, protection from noise. This allows a principled selection of the regularizer, and in particular, generalizations of Lasso that also yield convex optimization problems are obtained by considering different uncertainty sets. Second, robustness can itself be used as an avenue for exploring different properties of the solution. In particular, it is shown that robustness of the solution explains why the solution is sparse. The analysis as well as the specific results obtained differ from standard sparsity results, providing different geometric intuition. Furthermore, it is shown that the robust optimization formulation is related to kernel density estimation, and based on this approach, a proof that Lasso is consistent is given, using robustness directly. Finally, a theorem is proved which states that sparsity and algorithmic stability contradict each other, and hence Lasso is not stable. [J144]

"Codes in Permutations and Error Correction for Rank Modulation"

Codes for rank modulation have been recently proposed as a means of protecting flash memory devices from errors. We study basic coding theoretic problems for such codes, representing them as subsets of the set of permutations of nelements equipped with the Kendall tau distance. We derive several lower and upper bounds on the size of codes. These bounds enable us to establish the exact scaling of the size of optimal codes for large values of n. We also show the existence of codes whose size is within a constant factor of the sphere packing bound for any fixed number of errors. [J145]

"Dynamic FEC Algorithms for TFRC Flows"

Media flows coexist with TCP-based data traffic on the Internet and are required to be TCP-friendly. The TCP protocol slowly increases its sending rate until episodes of congestion occur, and then it quickly reduces its rate to remove congestion. However, media flows can be sensitive to even brief episodes of congestion. In this paper, we are interested in protecting media flows from TCP-induced congestion while maintaining their TCP friendliness. In particular, we consider media flows carried over the TCP-Friendly Rate Control (TFRC) protocol and we design algorithms that dynamically adapt the level of forward error correction (FEC) based on the congestion state of the network. To this end, first, we investigate the loss and delay characteristics of TFRC flows in several TCP-induced congestion scenarios, and we develop novel predictors of loss events based on packet delay information. Second, we use these predictors to dynamically adapt the level of FEC protection based on the predicted level of congestion. We show that this technique can significantly improve the overhead versus reliability trade-off compared to fixed FEC. Third, we select the FEC and original media packets within each FEC block, in a rate-distortion optimized way, and we show that this technique significantly improves media quality. [J146]

"Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel"

The role of multiple antennas for secure communication is investigated within the framework of Wyner's wiretap channel. We characterize the secrecy capacity in terms of generalized eigenvalues when the sender and eavesdropper have multiple antennas, the intended receiver has a single antenna, and the channel matrices are fixed and known to all the terminals, and show that a beamforming strategy is capacity-achieving. In addition, we study a masked beamforming scheme that radiates power isotropically in all directions and show that it attains near-optimal performance in the high SNR regime. Insights into the scaling behavior of the capacity in the large antenna regime as well as extensions to ergodic fading channels are also provided. [J147]

"An off-line dictionary attack on a simple three-party key exchange protocol"

Key exchange protocols allow two or more parties communicating over a public network to establish a common secret key called a session key. Due to their significance in building a secure communication channel, a number of key exchange protocols have been suggested over the years for a variety of settings. Among these is the so-

called S-3PAKE protocol proposed by Lu and Cao for password-authenticated key exchange in the three-party setting. In the current work, we are concerned with the password security of the S-3PAKE protocol. We first show that S-3PAKE is vulnerable to an off-line dictionary attack in which an attacker exhaustively enumerates all possible passwords in an off-line manner to determine the correct one. We then figure out how to eliminate the security vulnerability of S-3PAKE. [J148]

"Analyzing the Video Popularity Characteristics of Large-Scale User Generated Content Systems"

User generated content (UGC), now with millions of video producers and consumers, is reshaping the way people watch video and TV. In particular, UGC sites are creating new viewing patterns and social interactions, empowering users to be more creative, and generating new business opportunities. Compared to traditional video-on-demand (VoD) systems, UGC services allow users to request videos from a potentially unlimited selection in an asynchronous fashion. To better understand the impact of UGC services, we have analyzed the world's largest UGC VoD system, YouTube, and a popular similar system in Korea, Daum Videos. In this paper, we first empirically show how UGC services are fundamentally different from traditional VoD services. We then analyze the intrinsic statistical properties of UGC popularity distributions and discuss opportunities to leverage the latent demand for niche videos (or the so-called "the Long Tail" potential), which is not reached today due to information filtering or other system scarcity distortions. Based on traces collected across multiple days, we study the popularity lifetime of UGC videos and the relationship between requests and video age. Finally, we measure the level of content aliasing and illegal content in the system and show the problems aliasing creates in ranking the video popularity accurately. The results presented in this paper are crucial to understanding UGC VoD systems and may have major commercial and technical implications for site administrators and content owners. [J149]

"Cyclic Lowest Density MDS Array Codes"

Three new families of lowest density maximum-distance separable (MDS) array codes are constructed, which are cyclic or quasi-cyclic. In addition to their optimal redundancy (MDS) and optimal update complexity (lowest density), the symmetry offered by the new codes can be utilized for simplified implementation in storage applications. The proof of the code properties has an indirect structure: first MDS codes that are not cyclic are constructed, and then transformed to cyclic codes by a minimum-distance preserving transformation. [J150]

"MPEG-21 and Its Interoperability with Rights-Information Standards"

Because the DAC profile was designed to be a superset of the other known rights information standards, there should be no problem in representing the four rights information standards with the DAC profile. However, due to different expressiveness coverage of the other rights information standards, the reverse directional interoperability between the DAC profile and the other standards seems problematic. Moreover, the interoperability between the other rights information standards except for the DAC profile seems to be even more difficult to achieve in spite of potential needs from the digital home environment. Therefore, further study is required to support the possible bidirectional interoperability between the existing rights information standards as well as reverse directional interoperability between the DAC profile and other rights information standards. [J151]

"An AS-level overlay network for IP traceback"

Distributed denial of service attacks currently represent a serious threat to the appropriate operation of Internet services. To deal with this threat, we propose an overlay network that provides an IP-traceback scheme at the level of autonomous systems. Our proposed autonomous system-level IP-traceback system contrasts with previous works because it does not require a priori knowledge of the network topology and allows single-packet traceback and incremental deployment. Our first contribution is a new extension to the Border Gateway Protocol update-message community attribute that enables information to be passed across autonomous systems that are not necessarily involved in the overlay network. The second contribution is a new sequence-marking process to remove ambiguities in the traceback path. Two different strategies for incremental system deployment are investigated and evaluated. We show that strategic placement of the system on highly connected autonomous systems produces relevant results for IP traceback even if the system operates on only a few autonomous systems. The main conclusion is that the proposed system is suitable for large-scale networks such as the Internet because it provides efficient traceback and allows incremental deployment. [J152]

"ANGEL: Enhancing the Utility of Generalization for Privacy Preserving Publication"

Generalization is a well-known method for privacy preserving data publication. Despite its vast popularity, it has several drawbacks such as heavy information loss, difficulty of supporting marginal publication, and so on. To overcome these drawbacks, we develop ANGEL,1 a new anonymization technique that is as effective as

generalization in privacy protection, but is able to retain significantly more information in the microdata. ANGEL is applicable to any monotonic principles (e.g., l-diversity, t-closeness, etc.), with its superiority (in correlation preservation) especially obvious when tight privacy control must be enforced. We show that ANGEL lends itself elegantly to the hard problem of marginal publication. In particular, unlike generalization that can release only restricted marginals, our technique can be easily used to publish any marginals with strong privacy guarantees. [J153]

"Spatio-Temporal Just Noticeable Distortion Profile for Grey Scale Image/Video in DCT Domain"

In image and video processing field, an effective compression algorithm should remove not only the statistical redundancy information but also the perceptually insignificant component from the pictures. Just-noticeable distortion (JND) profile is an efficient model to represent those perceptual redundancies. Human eyes are usually not sensitive to the distortion below the JND threshold. In this paper, a DCT based JND model for monochrome pictures is proposed. This model incorporates the spatial contrast sensitivity function (CSF), the luminance adaptation effect, and the contrast masking effect based on block classification. Gamma correction is also considered to compensate the original luminance adaptation effect which gives more accurate results. In order to extend the proposed JND profile to video images, the temporal modulation factor is included by incorporating the temporal CSF and the eye movement compensation. Moreover, a psychophysical experiment was designed to parameterize the proposed model. Experimental results show that the proposed model is consistent with the human visual system (HVS). Compared with the other JND profiles, the proposed model can tolerate more distortion and has much better perceptual quality. This model can be easily applied in many related areas, such as compression, watermarking, error protection, perceptual distortion metric, and so on. [J154]

"A Graph Approach to Quantitative Analysis of Control-Flow Obfuscating Transformations"

Modern obfuscation techniques are intended to discourage reverse engineering and malicious tampering of software programs. We study control-flow obfuscation, which works by modifying the control flow of the program to be obfuscated, and observe that it is difficult to evaluate the robustness of these obfuscation techniques. In this paper, we present a framework for quantitative analysis of control-flow obfuscating transformations. Our framework is based upon the control-flow graph of the program, and we show that many existing control-flow obfuscation techniques can be expressed as a sequence of basic transformations on these graphs. We also propose a new measure of the difficulty of reversing these obfuscated programs, and we show that our framework can be used to easily evaluate the space penalty due to the transformations. [J155]

"Topological Analysis of Criminal Activity Networks: Enhancing Transportation Security"

The security of border and transportation systems is a critical component of the national strategy for homeland security. The security concerns at the border are not independent of law enforcement in border-area jurisdictions because the information known by local law enforcement agencies may provide valuable leads that are useful for securing the border and transportation infrastructure. The combined analysis of law enforcement information and data generated by vehicle license plate readers at international borders can be used to identify suspicious vehicles and people at ports of entry. This not only generates better quality leads for border protection agents but may also serve to reduce wait times for commerce, vehicles, and people as they cross the border. This paper explores the use of criminal activity networks (CANs) to analyze information from law enforcement and other sources to provide value for transportation and border security. We analyze the topological characteristics of CAN of individuals and vehicles in a multiple jurisdiction scenario. The advantages of exploring the relationships of individuals and vehicles are shown. We find that large narcotic networks are small world with short average path lengths ranging from 4.5 to 8.5 and have scale-free degree distributions with power law exponents of 0.85-1.3. In addition, we find that utilizing information from multiple jurisdictions provides higher quality leads by reducing the average shortest-path lengths. The inclusion of vehicular relationships and border-crossing information generates more investigative leads that can aid in securing the border and transportation infrastructure. [J156]

"Authentication Over Noisy Channels"

An authentication counterpart of Wyner's study of the wiretap channel is developed in this work. More specifically, message authentication over noisy channels is studied while impersonation and substitution attacks are investigated for both single- and multiple-message scenarios. For each scenario, information-theoretic lower and upper bounds on the opponent's success, or cheating, probability are derived. Remarkably, in both scenarios, the lower and upper bounds are shown to match, and hence, the fundamental limits on message authentication over noisy channels are fully characterized. The opponent's success probability is further shown to be smaller than that derived in the classical noiseless channel model. These results rely on a novel

authentication scheme in which shared key information is used to provide simultaneous protection against both types of attacks. Finally, message authentication for the case in which the source and receiver possess only correlated sequences is studied. [J157]

"Network access security in next- generation 3GPP systems: A tutorial"

The 3GPP Release 8 long term evolution/system architecture evolution marks the advancement of mobile cellular technology after UMTS-3G. The evolved packet system (EPS) architecture proposed in Release 8 introduces fundamental changes on top of UMTS in several design areas, including security. This article provides a tutorial overview of the proposed security mechanism in EPS. It first gives the background, a brief overview of the overall EPS architecture. It goes on to list the various requirements to be met for EPS security. A description of the EPS security architecture and detailed security procedures are given subsequently. The innovations that have been introduced in EPS, on top of UMTS, are highlighted all through the article. The article concludes by listing some open security issues at the moment. [J158]

"Driving Profile Modeling and Recognition Based on Soft Computing Approach"

Advancements in biometrics-based authentication have led to its increasing prominence and are being incorporated into everyday tasks. Existing vehicle security systems rely only on alarms or smart card as forms of protection. A biometric driver recognition system utilizing driving behaviors is a highly novel and personalized approach and could be incorporated into existing vehicle security system to form a multimodal identification system and offer a greater degree of multilevel protection. In this paper, detailed studies have been conducted to model individual driving behavior in order to identify features that may be efficiently and effectively used to profile each driver. Feature extraction techniques based on Gaussian mixture models (GMMs) are proposed and implemented. Features extracted from the accelerator and brake pedal pressure were then used as inputs to a fuzzy neural network (FNN) system to ascertain the identity of the driver. Two fuzzy neural networks, namely, the evolving fuzzy neural network (EFuNN) and the adaptive network-based fuzzy inference system (ANFIS), are used to demonstrate the viability of the two proposed feature extraction techniques. The performances were compared against an artificial neural network (NN) implementation using the multilayer perceptron (MLP) network and a statistical method based on the GMM. Extensive testing was conducted and the results show great potential in the use of the FNN for real-time driver identification and verification. In addition, the profiling of driver behaviors has numerous other potential applications for use by law enforcement and companies dealing with buses and truck drivers. [J159]

"One More Take on Identity"

After having just written two columns about identity, I'd like to change course by writing about ... identity. But there's a difference: my previous columns dealt mostly with how information available about us on the Internet has evolved in recent years. Here, I want to think a little more deeply about the methods we use to identify ourselves on the Internet-how we do it now, what's wrong with the current approach, and where this notion of identification might go in the future. [J160]

"On the Characterization and Optimization of On-Chip Cache Reliability against Soft Errors"

Soft errors induced by energetic particle strikes in on-chip cache memories have become an increasing challenge in designing new generation reliable microprocessors. Previous efforts have exploited information redundancy via parity/ECC codings or cacheline duplication for information integrity in on-chip cache memories. Due to various performance, area/size, and energy constraints in various target systems, many existing unoptimized protection schemes may eventually prove significantly inadequate and ineffective. In this paper, we propose a new framework for conducting comprehensive studies and characterization on the reliability behavior of cache memories, in order to provide insight into cache vulnerability to soft errors as well as design guidance to architects for highly efficient reliable on-chip cache memory design. Our work is based on the development of new lifetime models for data and tag arrays residing in both the data and instruction caches. Those models facilitate the characterization of cache vulnerability of stored items at various lifetime phases. We then exemplify this design methodology by proposing reliability schemes targeting at specific vulnerable phases. Benchmarking is carried out to showcase the effectiveness of our approach. [J161]

"State Estimation for the Localization of Harmonic Sources in Electric Distribution Systems"

Throughout the last years, with the liberalization of the energy market, the localization of the sources of power quality disturbances has become a nodal point for operators and customers. In the liberalized market, knowledge of the system status, along with the uncertainty affecting the estimated data, is required to operate management and control issues such as energy dispatching and protection coordination. In distribution systems, too many

measurement instruments would be needed to obtain a complete observation of the electric quantities. Thus, model-based state-estimation techniques can be implemented to exploit the few real-time measurements from the field and all the other available information to estimate the desired quantities. In this paper, a novel approach to the estimation of the harmonic sources by means of a Bayesian approach is proposed. The procedure also allows the ldquoqualityrdquo of the obtained estimates to be assessed. The theoretical fundamentals of the method are discussed, and results relevant to a simple distribution network are presented. [J162]

"Licensed or unlicensed: The economic considerations in incremental spectrum allocations"

At present, no existing market mechanism allows for the trading of radio spectrum between licensed and unlicensed uses. Whenever spectrum is made available for reallocation, the FCC faces a dilemma in determining which access regime to use. For example, the television white spaces are largely unused and available for reallocation. Since both licensed and unlicensed allocations are valuable, allocation decisions (for the TV white spaces or any new band of radio spectrum) must be based on a clear understanding of the trade-offs between the two choices. This article defines economic criteria that can be used in making these important decisions. Economic criteria can go beyond the simple measures of profit and consumer surplus from market transactions. Although some measures of benefit, such as the value of innovation, may be difficult to quantify, the analytic economic framework presented here can easily incorporate them. This analysis does not address any noneconomic considerations in choosing between licensed and unlicensed uses. As one example, the issue of potential societal benefits from promoting minority ownership of spectrum through restricted licenses-something only possible in a licensed regime-is not addressed in this economic analysis. The analysis herein provides the economic information needed for policy analysis; it need not be the sum total of that policy analysis. Standard economic theory tells us that the value of an additional unit of spectrum is equal to the increase in socially beneficial services it produces. For licensed spectrum allowed to trade in markets, this value is relatively easy to calculate: It is the price firms pay for the licensed spectrum. The equation is more complex, however, when unlicensed spectrum is involved. The current value of unlicensed spectrum bands is equal to the sum of the value of the spectrum in all uses in those bands. The incremental value of additional spectrum allocated to unlicensed uses, however, is based-on the relief to congestion the additional spectrum will provide. Unlicensed spectrum also contains a value associated with the possibility of future innovation made available by the lower transaction .costs of gaining access to unlicensed spectrum. This option value increases with additional allocations of unlicensed spectrum, leading to the benefit of incremental option value from additional unlicensed spectrum. The formula for the benefits from additional unlicensed spectrum allocations can be summarized as "congestion alleviation plus incremental option value." I apply the analysis developed in this article to the case of TV white spaces. I use information from the recent auction of the lower 700 MHz band E block to calculate the incremental value of licensing the white spaces. I also calibrate an estimate of the incremental value of the white spaces under an unlicensed allocation. Initial calibration of the economic criteria that determine the trade-off between incremental licensed and unlicensed spectrum allocations indicates that currently licensing incremental allocations is the favored policy. If policy makers choose to allocate incremental spectrum as unlicensed, they should recognize the economic costs of that choice. [J163]

"Approximation Bounds for Minimum Information Loss Microaggregation"

The NP-hard microaggregation problem seeks a partition of data points into groups of minimum specified size k, so as to minimize the sum of the squared euclidean distances of every point to its group's centroid. One recent heuristic provides an O(k3) guarantee for this objective function and an O(k2) guarantee for a version of the problem that seeks to minimize the sum of the distances of the points to its group's centroid. This paper establishes approximation bounds for another microaggregation heuristic, providing better approximation guarantees of O(k2) for the squared distance measure and O(k) for the distance measure. [J164]

"A Modified Matched Filter With Double-Sided Thresholding for Screening Proliferative Diabetic Retinopathy"

The early diagnosis of proliferative diabetic retinopathy (PDR), a common complication of diabetes that damages the retina, is crucial to the protection of the vision of diabetes sufferers. The onset of PDR is signaled by the appearance of neovascular net. Such neovascular nets might be identified using retinal vessel extraction techniques. The commonly used matched filter methods often produce false positive detections of neovascular nets due to their proneness to detect nonline edges as well as lines. In this paper, we propose a modified matched filter for retinal vessel extraction that applies a local vessel cross-section analysis using double-sided thresholding to reduce false responses to nonlinear edges. Our proposed modified matched filters demonstrated higher true positive rate and lesser false detection than existing matched-filter-based schemes in vessel extraction. [J165]

"Temperature Attacks"

Confining a program during its execution so that it can't leak information to other programs is an old concern. Recently, several researchers succeeded in fingerprinting distant machines by measuring temperature side effects on clocks. But can temperature also leak secrets in a computer or a chip? We started by implementing a covert channel between two processes (a sender and a receiver) running on the same machine. Producing heat is simple: all the sender must do is launch massive calculations. To sense temperature in the machine, we considered three options: fan-based solutions, built-in sensors; and faults as heat detectors. [J166]

"Integrated Digital Rights Management for Mobile IPTV Using Broadcasting and Communications"

This paper presents a digital rights management (DRM) scheme for mobile broadcasting that integrates management via broadcasting and communications. The scheme provides access control and rights protection for subscription Mobile IPTV (Internet Protocol TV), enabling transmission of contract information to control broadcasting reception via both broadcasting wave and communications. It has transmission functions that reduce the amount of contract information that has to be transmitted through broadcasting as well as a function for transmitting contract information via communications. A PC simulation indicates that the DRM scheme is effective in terms of the transmission rate required to send contract information via broadcasting wave. We also demonstrated the feasibility of the DRM scheme by using a prototype system implemented on an SIM card. The DRM scheme enables advanced mobile receiver functions such as pay-per-view with an interactivity channel using communications and a subscription TV such as pay-per-month on mobile receivers without an interactivity channel by transmitting contract information via broadcasting wave. [J167]

"Flexible Hardware Processor for Elliptic Curve Cryptography Over NIST Prime Fields"

Exchange of private information over a public medium must incorporate a method for data protection against unauthorized access. Elliptic curve cryptography (ECC) has become widely accepted as an efficient mechanism to secure sensitive data. The main ECC computation is a scalar multiplication, translating into an appropriate sequence of point operations, each involving several modular arithmetic operations. We describe a flexible hardware processor for performing computationally expensive modular addition, subtraction, multiplication, and inversion over prime finite fields GF(p) . The proposed processor supports all five primes precommended by NIST, whose sizes are 192, 224, 256, 384, and 521 bits. It can also be programmed to automatically execute sequences of modular arithmetic operations. Our field-programmable gate-array implementation runs at 60 MHz and takes between 4 and 40 ms (depending on the used prime) to perform a typical scalar multiplication. [J168]

"Performance Bounds for Unequal Error Protecting Turbo Codes"

In many communications systems, data can be divided into different importance levels. For these systems, unequal error protection (UEP) techniques are used to guarantee lower BER for the more important classes. In particular, if the precise characteristics of the channel are not known, UEP can be used to recover the more important classes even in poor receiving conditions. In this paper, we derive bounds on the performance of unequal error protecting turbo codes. These bounds serve as an important tool in predicting the performance of these codes. In order to derive the bounds, we introduce the notion of UEP uniform interleaver which is a random interleaver that does not change the order of classes in the turbo code frame. We also present a method to derive the weight enumerating function for UEP turbo codes. [J169]

"Fingerprint Verification Using Spectral Minutiae Representations"

Most fingerprint recognition systems are based on the use of a minutiae set, which is an unordered collection of minutiae locations and orientations suffering from various deformations such as translation, rotation, and scaling. The spectral minutiae representation introduced in this paper is a novel method to represent a minutiae set as a fixed-length feature vector, which is invariant to translation, and in which rotation and scaling become translations, so that they can be easily compensated for. These characteristics enable the combination of fingerprint recognition systems with template protection schemes that require a fixed-length feature vector. This paper introduces the concept of algorithms for two representation methods: the location-based spectral minutiae representation and the orientation-based spectral minutiae representation. Both algorithms are evaluated using two correlation-based spectral minutiae matching algorithms. We present the performance of our algorithms on three fingerprint databases. We also show how the performance can be improved by using a fusion scheme and singular points. [J170]

"Forward Error Correction for Multipath Media Streaming"

We address the problem of joint optimal rate allocation and scheduling between media source rate and error

protection rate in scalable streaming applications over lossy multipath networks. Starting from a distortion representation of the received media information at the client, we propose a novel optimization framework in which we analyze the performance of the most relevant forward error correction and scheduling techniques. We describe both optimal and heuristic algorithms that find solutions to the rate allocation and scheduling problem, and emphasize the main characteristics of the compared techniques. Our results show that efficient unequal error protection schemes improve the quality of the streaming process. At the same time we emphasize the importance of priority scheduling of the information over the best available network paths, which outperforms traditional first-in-first-out models or network flooding mechanisms. [J171]

"EXIT-Chart Optimized Short Block Codes for Iterative Joint Source and Channel Decoding in H.264 Video Telephony"

In this paper, we propose a family of short block codes (SBCs) designed for guaranteed convergence in soft-bit-assisted iterative joint source and channel decoding, which facilitate improved iterative soft-bit source decoding (SBSD) and channel decoding. Data-partitioned (DP) H.264 source-coded video is used to evaluate the performance of our system using SBC-assisted SBSD, in conjunction with recursive systematic convolution (RSC) codes for transmission over correlated narrow-band Rayleigh fading channels. The effect of different SBC schemes having diverse minimum Hamming distances dH,minand code rates on the attainable system performance is demonstrated, when using iterative SBSD and channel decoding, while keeping the overall bit rate budget constant by appropriately partitioning the total available bit rate budget between the source and channel codecs to improve the overall bit error rate (BER) performance and to enhance the objective video quality expressed in terms of peak signal-to-noise ratio (PSNR). EXtrinsic Information Transfer (EXIT) charts were used to analyze the attainable system performance. Explicitly, our experimental results show that the proposed error protection scheme using rate-1/3 SBCs having dH,min= 6 outperforms the identical-rate SBCs having dH,min= 3 by about 2.25 dB at the PSNR degradation point of 1 dB. Additionally, an Eb/N0gain of 9 dB was achieved, compared with the rate-5/6 SBC having dH,min= 2 and an identical overall code rate. Furthermore, an Eb/N0gain of 25 dB is attained at the PSNR degradation point of 1 dB while using iterative soft-bit source and channel decoding with the aid of rate-1/3 SBCs relative to the identical-rate benchmarker. [J172]

"Silver Bullet Talks with Jeremiah Grossman"

Silver Bullet Security Podcast host Gary McGraw interviews Jeremiah Grossman, founder and CTO of WhiteHat Security, who is well known for his work in Web application security. [J173]

"Mobile Human Airbag System for Fall Protection Using MEMS Sensors and Embedded SVM Classifier"

This paper introduces a mobile human airbag system designed for fall protection for the elderly. A Micro Inertial Measurement Unit (muIMU) of 56 mm times 23 mm times 15 mm in size is built. This unit consists of three dimensional MEMS accelerometers, gyroscopes, a Bluetooth module and a Micro Controller Unit (MCU). It records human motion information, and, through the analysis of falls using a high-speed camera, a lateral fall can be determined by gyro threshold. A human motion database that includes falls and other normal motions (walking, running, etc.) is set up. Using a support vector machine (SVM) training process, we can classify falls and other normal motions successfully with a SVM filter. Based on the SVM filter, an embedded digital signal processing (DSP) system is developed for real-time fall detection. In addition, a smart mechanical airbag deployment system is finalized. The response time for the mechanical trigger is 0.133 s, which allows enough time for compressed air to be released before a person falls to the ground. The integrated system is tested and the feasibility of the airbag system for real-time fall protection is demonstrated. [J174]

"De-Interlacing Algorithm Using Spatial-Temporal Correlation-Assisted Motion Estimation"

De-interlacing algorithms are used to convert interlaced video into progressive scanning format. The motion-adaptive technique provides acceptable picture quality, but the quality of the motion area still needs to be improved. Among the various de-interlacing techniques, the motion-compensated de-interlacing technique provides the best performance if the estimated motion information is reliable. However, it suffers from inaccurate motion estimation, and the weak error protection thus deteriorates the visual quality. This paper presents a motion-compensated de-interlacing algorithm with highly accurate motion estimation and robust error detection. In order to obtain more accurate motion information, spatial-temporal correlation-assisted motion estimation is proposed. The spatial and temporal correlations among the motion vectors (MVs) are exploited to find the true motion of the object. In order to reject incorrect temporal information, a hierarchical MV reliability verification is provided. The possible defects in both large and small areas can be detected effectively. The experimental results show that the proposed algorithm outperforms existing algorithms and produces high quality de-interlaced

results in various video sequences. [J175]

"Overview of Licensing and Legal Issues for Digital Forensic Investigators"

Digital forensic examiners face challenges outside the technical aspects of collecting, investigating, and storing digital information. Rules about admissibility and the licensing requirements for forensic professionals must also be taken into account. The use of digital data in an expanding number of US court cases and business investigations has precipitated changes in evidence handling and admissibility requirements, most notably in the 2006 changes to the Federal Rules of Civil Procedure. Knowledge of these rules and the ensuing case law is an essential component of any examiner's toolkit because improper evidence handling can lead to inadmissible evidence. The court's acceptance of such evidence is also greatly affected by the examiner's proper licensure. Unfortunately, these requirements vary by state (sometimes even by city) and are constantly changing. Therefore, digital forensic investigators must heed both the court's rules regarding evidence handling and the state's rules for licensing in order to be most effective. [J176]

"A New Era of Presidential Security: The President and His BlackBerry"

Americans are addicted to their personal digital assistants (PDAs), and President Barack Obama is no exception. Throughout the primaries and the presidential campaign, Obama was often seen using his BlackBerry. Once he won the election, great debate ensued as to whether he would be allowed to continue using it once in office. Initially, the secret service determined that his BlackBerry did not provide the requisite security required for its continued use. Of special concern was the potential that attackers could gain access to government work. Although Obama persuaded his security staff to let him keep using his BlackBerry (or a BlackBerry-like handheld device), it is not clear how, exactly, the device was modified to ensure extra security. [J177]

"Searching for You (review of Googling Security: How Much Does Google Know About You? by G. Conti; 2008) [JBook reviews]"

This book warns readers about the proliferation of data capture and the degree to which we're tracked and traced on the Web. In ten heavily illustrated chapters, the author explains how our data are captured, retained, and shared (often for a price) with third parties. The author dedicates a chapter to ways of addressing the threat. He suggests methods for controlling cookies, diffusing or eliminating disclosures, encrypting important data, protecting a network address, and using policy as well as technical devices to minimize data capture and retention. [J178]

"Forensics Is So "Yesterday""

Computer forensics' presumed usefulness against anyone with computer savvy is minimal because such persons can readily defeat forensics techniques. Because computer forensics can't show who put the data where forensics found it, it can be evidence of nothing. [J179]

"Robust Blind Watermarking of Point-Sampled Geometry"

Digital watermarking for copyright protection of 3-D meshes cannot be directly applied to point clouds, since we need to derive consistent connectivity information, which might change due to attacks, such as noise addition and cropping. Schemes for point clouds operate only on the geometric data and, hence, are generic and applicable to mesh-based representations of 3-D models. For building generic copyright schemes for 3-D models, this paper presents a robust blind watermarking mechanism for 3-D point-sampled geometry. The basic idea is to find a cluster tree from clusters of 3-D points. Using the cluster tree, watermarks can be embedded and extracted by deriving an order among points at global (intracluster) and local levels (intercluster). The multiple bit watermarks are encoded/decoded inside each cluster based on an extension of the cluster structure-based 3-D quantization index modulation. The encoding mechanism makes the technique robust against uniform affine transformations (rotation, scaling, and transformation), reordering, cropping, simplification, and noise addition attacks. The technique when applied to 3-D meshes also achieves robustness against retriangulation and progressive compression techniques. Customization of the bit-encoding scheme achieves high hiding capacity with embedding rates that are equal to 4 b/point, while maintaining the imperceptibility of the watermark with low distortions. The estimated time complexity is O(nlogn), where nis the number of 3-D points. [J180]

"Multirelational k-Anonymity"

k-anonymity protects privacy by ensuring that data cannot be linked to a single individual. In a k-anonymous data set, any identifying information occurs in at least k tuples. Much research has been done to modify a single-table data set to satisfy anonymity constraints. This paper extends the definitions of k-anonymity to multiple

relations and shows that previously proposed methodologies either fail to protect privacy or overly reduce the utility of the data in a multiple relation setting. We also propose two new clustering algorithms to achieve multirelational anonymity. Experiments show the effectiveness of the approach in terms of utility and efficiency. [J181]

"Engineering Privacy"

In this paper we integrate insights from diverse islands of research on electronic privacy to offer a holistic view of privacy engineering and a systematic structure for the discipline's topics. First we discuss privacy requirements grounded in both historic and contemporary perspectives on privacy. We use a three-layer model of user privacy concerns to relate them to system operations (data transfer, storage and processing) and examine their effects on user behavior. In the second part of the paper we develop guidelines for building privacy-friendly systems. We distinguish two approaches: "privacy-by-policy" and "privacy-by-architecture." The privacy-by-policy approach focuses on the implementation of the notice and choice principles of fair information practices (FIPs), while the privacy-by-architecture approach minimizes the collection of identifiable personal data and emphasizes anonymization and client-side data storage and processing. We discuss both approaches with a view to their technical overlaps and boundaries as well as to economic feasibility. The paper aims to introduce engineers and computer scientists to the privacy research domain and provide concrete guidance on how to design privacy-friendly systems. [J182]

"Privacy-Preserving Kth Element Score over Vertically Partitioned Data"

Given a large integer data set shared vertically by two parties, we consider the problem of securely computing a score separating the kth and the (k + 1) to compute such a score while revealing little additional information. The proposed protocol is implemented using the Fairplay system and experimental results are reported. We show a real application of this protocol as a component used in the secure processing of top-k queries over vertically partitioned data. [J183]

"Comparative Investigation of Tram Vibrations"

The aim of this paper is to investigate the vibrations in a new tram model (the ldquoCombino Plusrdquo) developed by Siemens Company, Germany, which was recently launched on a main Budapest road, and in an older tram model withdrawn from the same line. Comparative measurements were made from terminal to terminal (18 sections). The results of this investigation gave us information about the advances made in relation to the vibrational characteristics of trams. This paper summarizes literature concerning the physiological effects of continuous vibration exposures, as well as the standard ISO 2631, to clarify the relevance of the topic and to draw attention to the recorded parameters of the new ldquoCombino Plusrdquo tram. The new ldquoCombino Plusrdquo tram successfully absorbs the vibrations originating from the roughness of the tram rail. This tram produces significantly less vibration for passengers and drivers than the older model tram withdrawn from the main road traffic. The new Combino Plus satisfies the ergonomic requirements and ensures favorable working conditions. [J184]

"Provably Secure Steganography"

Steganography is the problem of hiding secret messages in "innocent-lookingrdquo public communication so that the presence of the secret messages cannot be detected. This paper introduces a cryptographic formalization of steganographic security in terms of computational indistinguishability from a channel, an indexed family of probability distributions on cover messages. We use cryptographic and complexity-theoretic proof techniques to show that the existence of one-way functions and the ability to sample from the channel are necessary conditions for secure steganography. We then construct a steganographic protocol, based on rejection sampling from the channel, that is provably secure and has nearly optimal bandwidth under these conditions. This is the first known example of a general provably secure steganographic protocol. We also give the first formalization of "robustrdquo steganography, where an adversary attempts to remove any hidden messages without unduly disrupting the cover channel. We give a necessary condition on the amount of disruption the adversary is allowed in terms of a worst case measure of mutual information. We give a construction that is provably secure and computationally efficient and has nearly optimal bandwidth, assuming repeatable access to the channel distribution. [J185]

"Shadow Enhancement in Synthetic Aperture Sonar Using Fixed Focusing"

A shadow cast by an object on the seafloor is important information for target recognition in synthetic aperture sonar (SAS) images. Synthetic aperture imaging causes a fundamental limitation to shadow clarity because the illuminator is moved during the data collection. This leads to a blend of echo and shadow, or geometrical fill-in

in the shadow region. The fill-in is most dominant for widebeam synthetic aperture imaging systems. By treating the shadow as a moving target and compensating for the motion during the synthetic aperture imagery, we avoid the geometrical shadow fill-in. We show this to be equivalent to fixing the focus at the range of the shadow caster. This novel technique, referred to as fixed focus shadow enhancement (FFSE) can be used directly as an imaging method on hydrophone data or as a postprocessing technique on the complex SAS image. We demonstrate the FFSE technique on simulated data and on real data from a rail-based SAS, and on two different SAS systems operated on a HUGIN autonomous underwater vehicle. [J186]

"Accurately Measuring Denial of Service in Simulation and Testbed Experiments"

Researchers in the denial-of-service (DoS) field lack accurate, quantitative, and versatile metrics to measure service denial in simulation and testbed experiments. Without such metrics, it is impossible to measure severity of various attacks, quantify success of proposed defenses, and compare their performance. Existing DoS metrics equate service denial with slow communication, low throughput, high resource utilization, and high loss rate. These metrics are not versatile because they fail to monitor all traffic parameters that signal service degradation. They are not quantitative because they fail to specify exact ranges of parameter values that correspond to good or poor service quality. Finally, they are not accurate since they were not proven to correspond to human perception of service denial. We propose several DoS impact metrics that measure the quality of service experienced by users during an attack. Our metrics are quantitative: they map QoS requirements for several applications into measurable traffic parameters with acceptable, scientifically determined thresholds. They are versatile: they apply to a wide range of attack scenarios, which we demonstrate via testbed experiments and simulations. We also prove metrics' accuracy through testing with human users. [J187]

"Visualization of Simulated Urban Spaces: Inferring Parameterized Generation of Streets, Parcels, and Aerial Imagery"

Urban simulation models and their visualization are used to help regional planning agencies evaluate alternative transportation investments, land use regulations, and environmental protection policies. Typical urban simulations provide spatially distributed data about number of inhabitants, land prices, traffic, and other variables. In this article, we build on a synergy of urban simulation, urban visualization, and computer graphics to automatically infer an urban layout for any time step of the simulation sequence. In addition to standard visualization tools, our method gathers data of the original street network, parcels, and aerial imagery and uses the available simulation results to infer changes to the original urban layout and produce a new and plausible layout for the simulation results. In contrast with previous work, our approach automatically updates the layout based on changes in the simulation data and thus can scale to a large simulation over many years. The method in this article offers a substantial step forward in building integrated visualization and behavioral simulation systems for use in community visioning, planning, and policy analysis. We demonstrate our method on several real cases using a 200-Gbyte database for a 16,300 km2area surrounding Seattle. [J188]

"Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis"

Joint analysis of security and routing protocols in wireless networks reveals vulnerabilities of secure network traffic that remain undetected when security and routing protocols are analyzed independently. We formulate a class of continuous metrics to evaluate the vulnerability of network traffic as a function of security and routing protocols used in wireless networks. We develop two complementary vulnerability definitions using set theoretic and circuit theoretic interpretations of the security of network traffic, allowing a network analyst or an adversary to determine weaknesses in the secure network. We formalize node capture attacks using the vulnerability metric as a nonlinear integer programming minimization problem and propose the GNAVE algorithm, a Greedy Node capture Approximation using Vulnerability Evaluation. We discuss the availability of security parameters to the adversary and show that unknown parameters can be estimated using probabilistic analysis. We demonstrate vulnerability evaluation using the proposed metrics and node capture attacks using the GNAVE algorithm through detailed examples and simulation. [J189]

"Dynamic Routing with Security Considerations"

Security has become one of the major issues for data communication over wired and wireless networks. Different from the past work on the designs of cryptography algorithms and system infrastructures, we aim at the proposing of a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as routing information protocol in wired networks and destination-sequenced distance vector protocol in wireless networks, without introducing extra control messages. An analytic study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the analytic results and to show the capability of the proposed

algorithm. [J190]

"Cryptanalysis of a New Ultralightweight RFID Authentication Protocol—SASI"

Since RFID tags are ubiquitous and at times even oblivious to the human user, all modern RFID protocols are designed to resist tracking so that the location privacy of the human RFID user is not violated. Another design criterion for RFIDs is the low computational effort required for tags, in view that most tags are passive devices that derive power from an RFID reader's signals. Along this vein, a class of ultralightweight RFID authentication protocols has been designed, which uses only the most basic bitwise and arithmetic operations like exclusive-OR, OR, addition, rotation, and so forth. In this paper, we analyze the security of the SASI protocol, a recently proposed ultralightweight RFID protocol with better claimed security than earlier protocols. We show that SASI does not achieve resistance to tracking, which is one of its design objectives. [J191]

"Detecting Malicious Packet Losses"

In this paper, we consider the problem of detecting whether a compromised router is maliciously manipulating its stream of packets. In particular, we are concerned with a simple yet effective attack in which a router selectively drops packets destined for some victim. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Previous detection protocols have tried to address this problem with a user-defined threshold: too many dropped packets imply malicious intent. However, this heuristic is fundamentally unsound; setting this threshold is, at best, an art and will certainly create unnecessary false positives or mask highly focused attacks. We have designed, developed, and implemented a compromised router detection protocol that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses that will occur. Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions. We have tested our protocol in Emulab and have studied its effectiveness in differentiating attacks from legitimate network behavior. [J192]

"A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study"

In mobile ad hoc networks (MANETs), many applications require group-oriented computing among a large number of nodes in an adversarial environment. To deploy these large-scale cooperative applications, secure multicast service must be provided to efficiently and safely exchange data among nodes. The existing literature has extensively studied security protection for a single multicast group, in which all nodes are assumed to have the same security level. However, such an assumption may not be valid in practice because, for many applications, different users can play different roles and thus naturally be classified into multiple security levels. In this paper, we propose a pyramidal security model to safeguard the multisecurity-level information sharing in one cooperation domain. As a prominent feature, a pyramidal security model contains a set of hierarchical security groups and multicast groups. To find an efficient key management solution that covers all the involved multicast groups, we develop the following three schemes for the proposed security model: (1) separated star key graph; (2) separated tree key graph, and (3) integrated tree key graph. Performance comparison demonstrates that the scheme of integrated tree key graph has advantages over its counterparts. [J193]

"k-Anonymization with Minimal Loss of Information"

The technique of k-anonymization allows the releasing of databases that contain personal information while ensuring some degree of individual privacy. Anonymization is usually performed by generalizing database entries. We formally study the concept of generalization, and propose three information-theoretic measures for capturing the amount of information that is lost during the anonymization process. The proposed measures are more general and more accurate than those that were proposed by Meyerson and Williams and Aggarwal et al. We study the problem of achieving k-anonymity with minimal loss of information. We prove that it is NP-hard and study polynomial approximations for the optimal solution. Our first algorithm gives an approximation guarantee of O(ln k) for two of our measures as well as for the previously studied measures. This improves the best-known O(k)-approximation in. While the previous approximation algorithms relied on the graph representation framework, our algorithm relies on a novel hypergraph representation that enables the improvement in the approximation ratio from O(k) to O(ln k). As the running time of the algorithm is O(n2k}), we also show how to adapt the algorithm in in order to obtain an O(k)-approximation algorithm that is polynomial in both nand k. [J194]

"Beyond Output Voting: Detecting Compromised Replicas Using HMM-Based Behavioral Distance"

Many host-based anomaly detection techniques have been proposed to detect code-injection attacks on servers.

The vast majority, however, are susceptible to "mimicry" attacks in which the injected code masquerades as the original server software, including returning the correct service responses, while conducting its attack. "Behavioral distance," by which two diverse replicas processing the same inputs are continually monitored to detect divergence in their low-level (system-call) behaviors and hence potentially the compromise of one of them, has been proposed for detecting mimicry attacks. In this paper, we present a novel approach to behavioral distance measurement using a new type of hidden Markov model, and present an architecture realizing this new approach. We evaluate the detection capability of this approach using synthetic workloads and recorded workloads of production Web and game servers, and show that it detects intrusions with substantially greater accuracy than a prior proposal on measuring behavioral distance. We also detail the design and implementation of a new architecture, which takes advantage of virtualization to measure behavioral distance. We apply our architecture to implement intrusion-tolerant Web and game servers, and through trace-driven simulations demonstrate that it experiences moderate performance costs even when thresholds are set to detect stealthy mimicry attacks. [J195]

"The Design of a Generic Intrusion-Tolerant Architecture for Web Servers"

Nowadays, more and more information systems are connected to the Internet and offer Web interfaces to the general public or to a restricted set of users. Such openness makes them likely targets for intruders, and conventional protection techniques have been shown insufficient to prevent all intrusions in such open systems. This paper proposes a generic architecture to implement intrusion-tolerant Web servers. This architecture is based on redundancy and diversification principles in order to increase the system resilience to attacks: usually, an attack targets a particular software, running on a particular platform, and fails on others. The architecture is composed of redundant proxies that mediate client requests to a redundant bank of diversified application servers. The redundancy is deployed here to increase system availability and integrity. To improve performance, adaptive redundancy is applied: the redundancy level is selected according to the current alert level. The architecture can be used for static servers, that is, for Web distribution of stable information (updated offline) and for fully dynamic systems where information updates are executed immediately on an online database. The feasibility of this architecture has been demonstrated by implementing an example of a travel agency Web server, and the first performance tests are satisfactory, both for request execution times and recovery after incidents. [J196]

"Multiple Routing Configurations for Fast IP Network Recovery"

As the Internet takes an increasingly central role in our communications infrastructure, the slow convergence of routing protocols after a network failure becomes a growing problem. To assure fast recovery from link and node failures in IP networks, we present a new recovery scheme called Multiple Routing Configurations (MRC). Our proposed scheme guarantees recovery in all single failure scenarios, using a single mechanism to handle both link and node failures, and without knowing the root cause of the failure. MRC is strictly connectionless, and assumes only destination based hop-by-hop forwarding. MRC is based on keeping additional routing information in the routers, and allows packet forwarding to continue on an alternative output link immediately after the detection of a failure. It can be implemented with only minor changes to existing solutions. In this paper we present MRC, and analyze its performance with respect to scalability, backup path lengths, and load distribution after a failure. We also show how an estimate of the traffic demands in the network can be used to improve the distribution of the recovered traffic, and thus reduce the chances of congestion when MRC is used. [J197]

"Privacy-Aware Collaborative Spam Filtering"

While the concept of collaboration provides a natural defense against massive spam e-mails directed at large numbers of recipients, designing effective collaborative anti-spam systems raises several important research challenges. First and foremost, since e-mails may contain confidential information, any collaborative anti-spam approach has to guarantee strong privacy protection to the participating entities. Second, the continuously evolving nature of spam demands the collaborative techniques to be resilient to various kinds of camouflage attacks. Third, the collaboration has to be lightweight, efficient, and scalable. Toward addressing these challenges, this paper presents ALPACAS-a privacy-aware framework for collaborative spam filtering. In designing the ALPACAS framework, we make two unique contributions. The first is a feature-preserving message transformation technique that is highly resilient against the latest kinds of spam attacks. The second is a privacy-preserving protocol that provides enhanced privacy guarantees to the participating entities. Our experimental results conducted on a real e-mail data set shows that the proposed framework provides a 10 fold improvement in the false negative rate over the Bayesian-based Bogofilter when faced with one of the recent kinds of spam attacks. Further, the privacy breaches are extremely rare. This demonstrates the strong privacy protection provided by the ALPACAS system. [J198]

"Secured MyVirtualPDA using advanced encryption standard"

One of the most useful features in any personal digital assistant (PDA) is that it can accumulate information needed including easy-to-forget details. Some of the information stored is likely to be very sensitive including credit card numbers, personal identification, and passwords. To protect this sensitive data, most PDAs offer password protection as a basic authentication. However, to rely on this type of protection alone is not enough. As the writing of secret message cryptography, also known as science and mathematical lock and key (Schafer, 2003), evolved people rely on the encryption process to increase their level of data protection. [J199]

"Body Area Sensor Networks: Challenges and Opportunities"

Body area sensors can enable novel applications in and beyond healthcare, but research must address obstacles such as size, cost, compatibility, and perceived value before networks that use such sensors can become widespread. [J200]

"On the Security of Route Discovery in MANETs"

Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view. Recently, a security model tailored to the specific requirements of MANETs was introduced by Acs, Buttyan, and Vajda. Among the novel characteristics of this security model is that it promises security guarantee under concurrent executions, a feature of crucial practical implication for this type of distributed computation. A novel route discovery algorithm called endairA was also proposed, together with a claimed security proof within the same model. In this paper, we show that the security proof for the route discovery algorithm endairA is flawed, and moreover, this algorithm is vulnerable to a hidden channel attack. We also analyze the security framework that was used for route discovery and argue that composability is an essential feature for ubiquitous applications. We conclude by discussing some of the major security challenges for route discovery in MANETs. [J201]

"Surveying secure processors"

Secure computing is gaining importance as computing capability is increasingly becoming distributed and information is available everywhere. Prevention of piracy and digital rights management have become very important and information security is now mandatory rather than an additional feature. Various software schemes have been proposed to provide certain levels of copyright and intellectual property protection but are not completely safe from determined hackers. This has resulted in the need for information security at the hardware level, where secure processors assume importance. Keeping in view these new trends in computing, we review a few representative secure processor designs that are currently in industry and academia. The goal is to present the advantages and pitfalls of various secure processor designs and suggest possible enhancements to the existing secure processor architectures. [J202]

"Introducing "Insecure IT""

This article introduces "insecure IT", a new department for IT Professional that will cover security weaknesses in IT systems, ranging from desktops to global e-commerce networks. This regular feature will offer ideas to improve IT security, both by looking at ways it can go wrong as well as by covering good practices. [J203]

"The NRC Takes on Data Mining, Behavioral Surveillance, and Privacy"

In mid 2000, The Wall Street Journal reported that the US Federal Bureau of Investigation (FBI) was developing a tool for wiretapping at an Internet service provider (ISP). Carnivore, later renamed DCS 1000, was built to capture communications content-email,pages, and so forth-or the transactional information in the communications of targeted suspects. [J204]

"Teaching for Conceptual Change in Security Awareness: A Case Study in Higher Education"

In educational psychology, conceptual change is a process that revises a student's understanding of a topic in response to new information. Conceptual change pedagogy is particularly effective for security awareness education because instructors must deliver concepts to people who primarily just use computer networks and information systems rather than display expertise in the underlying technology. [J205]

"Silver Bullet Security Podcast Series"

{no data available} [J206]

"URBE: Web Service Retrieval Based on Similarity Evaluation"

In this work, we present UDDI registry by example (Urbe), a novel approach for Web service retrieval based on the evaluation of similarity between Web service interfaces. Our approach assumes that the Web service interfaces are defined with Web service description language (WSDL) and the algorithm combines the analysis of their structures and the analysis of the terms used inside them. The higher the similarity, the less are the differences among their interfaces. As a consequence, Urbe is useful when we need to find a Web service suitable to replace an existing one that fails. Especially in autonomic systems, this situation is very common since we need to ensure the self-management, the self-configuration, the self-optimization, the self-healing, and the self-protection of the application that is based on the failed Web service. A semantic-oriented variant of the approach is also proposed, where we take advantage of annotations semantically enriching WSDL specifications. Semantic Annotation for WSDL (SAWSDL) is adopted as a language to annotate a WSDL description. The Urbe approach has been implemented in a prototype that extends a universal description, discovery and integration (UDDI) compliant Web service registry. [J207]

"New principle for transmission line protection using phase portrait plane"

Phase portraits are a powerful mathematical model for describing oriented textures. An isotangent-based approach in a phase portrait is introduced to discriminate between internal and external faults. The scheme described is new and is a different approach to the problem of relaying ground faults on transmission lines. The geometrical theory of differential equations is used to drive a symbol set on the basis of the visual appearance of phase portraits. The dasiaphase portraitdasia of the instantaneous rate of change of current against voltage gives valuable information on the transient and stability characteristics of system configuration with high fault resistance and shunt susceptance of the transmission lines. Hundred percent of the protected zone is successfully discriminated rather than the external zone. An additional parameter that is considered, which is sometimes neglected in protection studies, is the shunt susceptance of the transmission lines. [J208]

"Better Binary List Decodable Codes Via Multilevel Concatenation"

A polynomial time construction of binary codes with the currently best known tradeoff between rate and error-correction radius is given. Specifically, linear codes over fixed alphabets are constructed that can be list decoded in polynomial time up to the so-called Blokh-Zyablov bound. The work builds upon earlier work by the authors where codes list decodable up to the Zyablov bound (the standard product bound on distance of concatenated codes) were constructed. The new codes are constructed via a (known) generalization of code concatenation called multilevel code concatenation. A probabilistic argument, which is also derandomized via conditional expectations, is used to show the existence of inner codes with a certain nested list decodability property that is appropriate for use in multilevel concatenated codes. A ldquolevel-by-levelrdquo decoding algorithm, which crucially uses the list recovery algorithm for the outer folded Reed-Solomon codes, enables list decoding up to the designed distance bound, aka the Blokh-Zyablov bound, for multilevel concatenated codes. [J209]

"Principles and Implementations of Hierarchical Region Defensive Systems of Power Grid"

A hierarchical region defensive system (RDS) based on optical fiber communications is proposed in this paper. This system comprises three layers. The bottom layer is the local measuring unit (LMU), which is equipped in those corresponding substations within this region. The intermediate layer is region decision layer comprising region decision units (RDUs). Every RDS has one RDU, which is connected with all LMUs within this region by means of optic fibers. The system monitor center on the top layer is mainly responsible for harmonizing and monitoring every RDU, recording the fault occurrences and adjusting the protection settings. This system offers safeguard to key region where energy converges inside the power network utilizing multipoint information, which cooperates with conventional main and backup protections. The hierarchical structure and operating principle has been detailed elaborated, especially the working process of measuring elements and decision-making elements. Various complicated fault scenarios within and out of the protected region are simulated using Electromagnetic Transients Program software to validate the proposed defensive system, and the results approve the correction of this system. Finally, the implementation of prototype of region protection system and the scenarios of dynamic simulation tests are provided. [J210]

"Seed-oil-based coolants for transformers"

This article presents information on the safety, reliability, and environmental performance of natural ester

transformer fluids by acquainting the readers with the history of transformer fluids and also explores how the industry has arrived at the current technologies of natural ester fluid. The properties of natural ester fluids are explained and then compared side by side with conventional mineral oil fluid. This article outlines two refinery case studies. The first case study is from a refinery in Texas City, where natural ester transformers were chosen for a new wet gas scrubber project. The second case study is from a refinery in Memphis, Tennessee, where natural ester fluid was used to retrofill an in-service, large-power transformer. These two case studies show the applicability of natural ester fluids in new and retrofilled distribution and power class transformers. [J211]

"Lightning-Induced Overvoltages Transferred Through Distribution Power Transformers"

This paper deals with the calculation of lightning-induced overvoltages on medium-voltage (MV) and low-voltage (LV) distribution networks taking into account the presence of MV-LV distribution transformers and, in particular, the surge transfer through them. The influence of the high-frequency model adopted for the representation of the power transformer on the calculation results is analyzed, with regards to two different models, both identified and validated by means of laboratory measurements: namely, a simple pi of capacitances, and the more complex one introduced by Morched, Marti, and Ottevangers in 1993. Accurate simulation results provide information on the adequacy of both models for the calculations of interest. Additional results, useful to evaluate the expected level of power quality and the benefits achievable by a proper installation of protection devices, are presented making reference to a realistic and complex configuration of an overhead distribution system. [J212]

"Quality of service for multimedia traffic using cross-layer design"

Quality-of-service (QoS) guarantees are critical for the transmission of multimedia traffic over mobile wireless networks. Currently, wireless networks provide QoS guarantees using the legacy layered protocol architecture where each layer provides a separate, independent solution, with its own optimised adaptation and protection mechanisms. Cross-layer design has been proposed as a methodology to extend that paradigm in wireless links where there is interdependence between the layers and hence opportunity for information sharing. Recently, cross-layer adaptation mechanisms have been proposed which attempt to solve the QoS provisioning problem. However, most of these mechanisms only use the lower (physical and data link) layers and the possibility of using higher protocol layers remains unexplored. As a result, restrictions are placed on the system which introduces functional and efficiency limitations. Here, one such limitation is highlighted, namely the inability to insert more than one class of traffic in a physical layer frame. A physical and application layer cross-layer adaptation mechanism is then proposed, which overcomes this limitation. The performance results of the scheme show that the cross-layer mechanism can be efficiently applied for the purpose of providing QoS guarantees for multimedia traffic. [J213]

"Statistical Analysis of Second Order Differential Power Analysis"

Second order Differential Power Analysis (2O-DPA) is a powerful side-channel attack that allows an attacker to bypass the widely used masking countermeasure. To thwart 2O-DPA, higher order masking may be employed but it implies a nonnegligible overhead. In this context, there is a need to know how efficient a 2O-DPA can be, in order to evaluate the resistance of an implementation that uses first order masking and, possibly, some hardware countermeasures. Different methods of mounting a practical 2O-DPA attack have been proposed in the literature. However, it is not yet clear which of these methods is the most efficient. In this paper, we give a formal description of the higher order DPA that are mounted against software implementations. We then introduce a framework in which the attack efficiencies may be compared. The attacks we focus on involve the combining of several leakage signals and the computation of correlation coefficients to discriminate the wrong key hypotheses. In the second part of this paper, we pay particular attention to 2O-DPA that involves the product combining or the absolute difference combining. We study them under the assumption that the device leaks the Hamming weight of the processed data together with an independent Gaussian noise. After showing a way to improve the product combining, we argue that in this model, the product combining is more efficient not only than absolute difference combining, but also than all the other combining techniques proposed in the literature. [J214]

"The Modeling and Verification of Peer-to-Peer Negotiating Multiagent Colored Petri Nets for Wide-Area Backup Protection"

This paper focuses on the modeling and verification of a peer-to-peer wide-area backup protection (WABP) system. Agents located in a number of substation intelligent electronic devices (IEDs) negotiate on a peer, or equal, basis. The agent-based wide-area backup protection scheme is able to find power-line faults and protection misoperations. A wide-area communication network based on IP technology is used to transmit shared information among the agents. A novel agent-oriented peer-to-peer negotiating colored Petri net

(AOPCPN) is proposed to implement the WABP system. The algorithms, design, and dynamic behavior of the WABP is evaluated in a simulated environment to demonstrate its benefits. The article begins by presenting the generic AOPCPN architecture and its formal definition. The AOPCPN model for the WABP multiagent system is evaluated according to one algorithm, which is detailed in this article. The WABP agent's autonomy, cooperation, parallel operation, and robustness are embodied in modules in order to ease the software engineering challenges in implementing and maintaining the agents. Three example scenarios illustrate the effectiveness of the Petri net model and its ability to dynamically respond to WABP misoperations and fault conditions. [J215]

"Silver Bullet Security Podcast series"

{no data available} [J216]

"The Application-View Model of the International Standard IEC 61850"

The introduction of IEC 61850 as the de facto SA standard for the communication between devices in a substation and the related system requirements has made it possible and justifiable to integrate station Intelligent Electronic Devices (IEDs) on a high-speed peer-to-peer communication network (Ethernet) through standardization. IEC 61850 presents a set of standard object-oriented (OO) data models to describe the processes to be implemented and controlled in a substation and a set of service models for the interactions between devices in a substation and the transfer of all sorts of IED data. IEC 61850 proposes the concept of standardizing IED data using data objects referred to as logical nodes. This makes it possible to achieve the ldquoplug and playrdquo capability so that information and commands can be shared on a single network independent from any implementation. In this paper, the authors describe the standard's application-view model and present the use of OO methodology and techniques for the implementation of the Logical Node (LN) application-view data model of the standard. The target audience for this paper includes power system protection and automation engineers and technicians as well as research personnel who have at least a basic understanding of the IEC 61850 international standard and other technology mechanisms addressed in this paper. [J217]

"Test-Driven Development for Spreadsheet Risk Management"

Spreadsheet technology is central to the functioning of the financial sector, but the spreadsheets themselves can have a high level of error that requires innovative supporting processes and tools. Several large-scale international studies conducted in response to the Enron-inspired Sarbanes-Oxley Act confirm the importance and complexity of spreadsheet systems in financial reporting, with some companies using 200+ spreadsheets in manually controlled interconnected "webs." Unfortunately, spreadsheets frequently have an unacceptably high number of faults. Early research indicated that between 2 and 5 percent of cell formulas can be incorrect, but a more recent study found that of 50 real-world operational spreadsheets audited, 94 percent contained errors with almost 1 percent of formula cells found to be incorrect. Spreadsheet developers don't appreciate this high risk and thus use little or no formal software development processes. [J218]

"Trust in M2M communication"

Machine-to-machine (M2M) communication is viewed as one of the next frontiers in wireless communications. M2M communication applications and scenarios are growing and lead the way to new business cases. Because of the nature of M2M scenarios, involving unguarded, distributed devices, new security threats emerge. The use case scenarios for M2M communication also address the new requirement on flexibility, because of deployment scenarios of the M2ME in the field. We believe that these new requirements require a paradigm shift. One important pillar of such a shift will be a new, more balanced mix of device-centric trust and traditional enforcement of security properties. [J219]

"Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks"

Large-scale bandwidth-based distributed denial-of-service (DDoS) attacks can quickly knock out substantial parts of a network before reactive defenses can respond. Even traffic that is not under direct attack can suffer significant collateral damage if the traffic passes through links that are common to attack routes. This paper presents a proactive surge protection (PSP) mechanism that aims to provide a broad first line of defense against DDoS attacks. The approach aims to minimize collateral damage by providing bandwidth isolation between traffic flows. The proposed solution is readily deployable using existing router mechanisms and does not rely on any unauthenticated packet header information. Our extensive evaluation across two large commercial backbone networks, using both distributed and targeted attacks, shows that up to 95.5% of the network could suffer collateral damage, but our solution was able to significantly reduce the amount of collateral damage by up to 97.58% in terms of the number of packets dropped and 90.36% in terms of the number of flows with packet

loss. Further, we show that PSP can maintain low packet loss rates even when the intensity of attacks is increased significantly. [J220]

"One-Wayness Equivalent to General Factoring"

This paper shows the first practical semantically secure public-key encryption scheme such that its one-wayness is equivalent to generalfactoring in the standardmodel [in the sense of indistinguishability against chosen-plaintext attack (IND-CPA)]. Next our proof technique is applied to the Rabin-Paillier encryption scheme and a variant of the RSA-Paillier encryption scheme to prove their one-wayness under the factoring assumption via tight security reductions. [J221]

"Knowledge sharing and diffusion patterns"

The international interrepository knowledge sharing and diffusion patterns in nanotechnology by analyzing patent publication trends from different national or regional repositories with particular focus on the most active countries and regions are presented. The data are collected from esp@cenet worldwide database, which holds more than 60 million patent documents published by patent offices in 85 countries. In conclusion, the patent applications from the esp@cenet worldwide database shows a great increase in global nanotechnology R&D output over the past three decades. [J222]

"Keyloggers"

Keyloggers are powerful tools that can perform many task. Standard security measures for machine-to-machine interfaces do not protect computer systems from keylogger attacks. Human-to-machine interfaces must be considered to combat keylogger intrusions. The judicious use of keyloggers by employers and computer owners could, in some situations, improve security, privacy, and efficiency. But the possible positive effects must be balanced against the possible negative effects on employees, users, and children. [J223]

"Privacy management service contacts as business opportunity"

The article discusses the service level agreement (SLA) and the privacy aspect. Economic and business considerations around privacy, and privacy of information in general have different levels of analysis and enforcement, as mentioned in the article. Economic and business considerations, require economic and business value to be defined and transacted upon. It should also be stressed that legal aspects are essential, as they may determine the nature of some privacy features as well as limits. Legal aspects obviously also apply to the fulfillment of the transactions between the economic individual and economic agents, directly or indirectly. The paper defines the framework and implementation of SLA management for privacy, as well as privacy metrics. A case study implementation in Cisco was mentioned. This article recognizes that privacy SLA's business value does not extend to all domains. But there are application domains where their introduction would be a major incentive scheme to increase controlled information and business interactions. [J224]

"A Hybrid Conditions-Dependent Outage Model of a Transformer in Reliability Evaluation"

Constant failure rate model used in the conventional reliability assessment of power systems cannot reflect the impacts of the various operating conditions such as transformer loading, ambient temperature, weather on component reliability. A hybrid conditions-dependent outage model (CDOM) of a transformer is proposed in this paper to include those impacts. The CDOM is the combination of three failure models: the aging failures due to the loss of mechanical strength of conductor insulation; the random failures considering weather conditions, and the outages caused by the direct trips of the overload protections. The component reliability using the proposed model has been tested under different operating conditions. The model is also applied in power system operational reliability assessment. The reliability indices using CDOM are compared with that using the condition-independent outage model. The reliability indices using the CDOMs of transformers can provide useful information for operators to understand possible system and component failure risk in real-time operation and to make important alleviation decisions. [J225]

"Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics"

A three-factor authentication scheme combines biometrics with passwords and smart cards to provide high-security remote authentication. Most existing schemes, however, rely on smart cards to verify biometric characteristics. The advantage of this approach is that the user's biometric data is not shared with remote server. But the disadvantage is that the remote server must trust the smart card to perform proper authentication which leads to various vulnerabilities. To achieve truly secure three-factor authentication, a method must keep

the user's biometrics secret while still allowing the server to perform its own authentication. Our method achieves this. The proposed scheme fully preserves the privacy of the biometric data of every user, that is, the scheme does not reveal the biometric data to anyone else, including the remote servers. We demonstrate the completeness of the proposed scheme through the GNY (Gong, Needham, and Yahalom) logic. Furthermore, the security of our proposed scheme is proven through Bellare and Rogaway's model. As a further benefit, we point out that our method reduces the computation cost for the smart card. [J226]

"Making the Best Use of Cybersecurity Economic Models"

This article describes an analysis of several representative cybersecurity economic models, where the authors seek to determine whether each model's underlying assumptions are realistic and useful. They find that many of the assumptions are the same across disparate models, and most assumptions are far from realistic. They recommend several changes so that the predictions from economic models can be more relevant and useful. [J227]

"Human Relationships: A Never-Ending Security Education Challenge?"

Even with high usability of security measures, well-trained and loyal employees don't always behave according to security guidance and may thus represent a security risk. This unexpected behavior is explained by a chain of barriers that employees must overcome to achieve a compliant behavior with security policy requirements. The findings the author reports here open up a discussion on how current information security education might benefit from including more subjects on the human factor. [J228]

"Disposal of Disk and Tape Data by Secure Sanitization"

User data is often unprotected on disk and tape drives or not erased when no longer needed, creating data security vulnerabilities that many computer users are unaware of. Federal and state laws require data sanitization, which comprises a variety of data eradication methods. Secure sanitization refers to methods meeting those federal and state laws. Companies that fail to meet these laws can be subject to fines of $5 million, and individuals can be imprisoned for up to 10 years. Physical destruction of storage devices offers the highest security. But executing the disk drive internal secure-erase command also offers a higher security level than external-block-overwrite software, according to federal guideline NIST 800-88. Recent disk drives with internal full disk encryption now implement an enhanced secure-erase command that takes only milliseconds to complete. [J229]

"Privacy-Aware Role-Based Access Control"

A privacy-aware role-based access control model extends RBAC to express highly complex privacy-related policies, including consideration of such features as conditions and obligations. Because it's based on the RBAC model, the full-fledged P-RBAC solution is easy to deploy in systems already adopting RBAC, thus allowing seamless integration of access control and privacy policies. [J230]

"Predictable Surprises"

Justifying security expenditures in difficult economic times is problematic at best, career ending at worst. This article provides a methodology to improve the probability of budget success based on risk assessment techniques, proven project management skills, and economics. [J231]

"Redundancy vs. Protection in Defending Parallel Systems Against Unintentional and Intentional Impacts"

This article considers defense resource allocation in a 1-out-of-N system exposed to external intentional impacts caused by malicious attacks, and unintentional impacts caused by naturally-occurring events or technological accidents. The defender distributes its resource between deploying redundant elements, and their protection. Two cases of the protection are considered: general protections that protect from both intentional, and unintentional impacts; and special protections of two different types that protect either against the intentional impacts, or against the unintentional impacts. Different combinations of intentional and unintentional impact sequences are considered. If the unintentional impact occurs first, the strategic attacker has full information about the elements destroyed, and concentrates all its effort on attacking only the survived elements. The vulnerability of each element is determined by contest success functions, between the defender and the attacker, and between the defender and the unintentional impact. A model, and a methodology for finding the defense resource distribution that minimizes the overall system vulnerability are suggested. Illustrative examples of the optimal defense are presented. [J232]

"GEANT4 Transport Calculations for Neutrons and Photons Below 15 MeV"

Neutron transport calculations are needed in many fields of radiation protection and medical physics. Neutron transport is often simulated with a Monte Carlo code, which allows the calculation of neutron dose distributions in different geometries, for example in voxel phantoms. So far little information is available about neutron transport below 15 MeV in tissue-like matter performed with the Monte Carlo code GEANT4. Therefore, we compared GEANT4 results of the ambient dose equivalent for neutron energies from 10 meV to 15 MeV with MCNP results and values published in ICRU 57. The GEANT4 code was found to be appropriate to calculate neutron and photon dose at energies below 15 MeV correctly. Furthermore, a method how to include a dose-assessment factor into the calculation was developed and tested. [J233]

"Optimizing Sensing: From Water to the Web"

Where should we place sensors to quickly detect contamination in drinking water distribution networks? Which blogs should we read to learn about the biggest stories on the Web? Such problems are typically NP-hard in theory and extremely challenging in practice. The authors present algorithms that exploit submodularity to efficiently find provably near-optimal solutions to large complex real-world sensing problems. [J234]

"Fighting the fakes [Janalysis]"

Summary form only given. The paper mentions that counterfeit components are a continuing headache for the electronics industry. The UK Electronics Alliance intends to launch a website to let engineers share information on fake components in an attempt to stem the flow of damaging counterfeits from the Far East. [J235]

"Surviving Distributed Denial-of-Service Attacks"

Business organizations and government agencies that depend on an Internet presence but operate without effective DDoS protection mechanisms put their operations at unacceptable risk. Unfortunately, the varieties of DDoS attacks, the incomplete information we have about them, the difficulty of large-scale testing, and the need for a distributed response at many points make defending against DDoS attacks a challenge. Because no silver bullet exists, businesses and government entities should have comprehensive mechanisms in place if they hope to prevent an attack-or failing that, survive one. [J236]

"Who Was James Clerk Maxwell and What Was and Is His Electromagnetic Theory?"

The electromagnetics community makes profuse utilization of Maxwell's equations, his theory, and their applications. It is arguable that very few of us have clear ideas about what exactly Maxwell did and what kind of scientist he was. In fact, he developed many of the fundamental ideas in electrical engineering, and provided mathematical language for their exposition. His contributions to other branches of science are no less significant. He was not only one of the great scientists of the nineteenth century, but was also great for all time. To this end, the present essay starts with a brief outline of his life. It then provides a short but critical discussion of his original contributions in electromagnetics and their evolution as his electromagnetic theory. We also give a cursory review of his significant contributions in other areas of science. It is hoped that this will provide the electromagnetics-community readers with a better and more complete appreciation of James Clerk Maxwell as a scientist, as well as of his electromagnetic theory as we know now it. [J237]

"Positive train control for Australia"

This article has provided a summary overview of the ATMS PTC system being developed for the ARTC. Discussed herein is the phased approach being taken to develop and roll out the system in the project territory. A system overview and system architecture description as well as a description of each of the major subsystems have been provided. ATMS can provide substantial operational benefits as outlined herein, and benefits that can be similarly realized in both domestic and foreign rail applications, and for both passenger and freight trains or a mixed combination of operations. The system provides a means of automating rail movements and increasing both system capacity and network velocity. Additional information on the ARTC and the ATMS can be found at the Web site http://www.artc.com.au. [J238]

"Advanced Unloading Analysis Considering Lateral Velocity and Disk RPM Drop in Emergency Parking"

A conventional unloading analysis was carried out in no consideration for fast lateral velocity and disk rpm drop during the emergency parking. However, current hard disk drive (HDD) systems need an improved performance

in the portable aspect. Therefore, much faster emergency parking is absolutely necessary to protect the system from sudden power-off or an external shock. In case of fast emergency parking, the fast lateral velocity causes an effective skew, and then there is a flying height (FH) loss which does not occur in a normal unload. Also, the FH loss induced by a disk rpm drop occurs at an unloading point in case that a portable small form factor HDD like 1.8 in is suddenly parking from inner diameter to outer diameter. This means that the unloading performance considering the effective skew becomes lower than one of the conventional unloading analysis. In this paper, we propose the advanced unloading analysis that can be applied to the fast emergency parking velocity. To do so, we investigate the FH loss by the fast lateral velocity and the disk rpm drop, and introduce the result of the advanced unloading analysis. [J239]

"Unequal Error Protection: An Information-Theoretic Perspective"

An information-theoretic framework for unequal error protection is developed in terms of the exponential error bounds. The fundamental difference between the bit-wiseand message-wiseunequal error protection (UEP) is demonstrated, for fixed-length block codes on discrete memoryless channels (DMCs) without feedback. Effect of feedback is investigated via variable-length block codes. It is shown that, feedback results in a significant improvement in both bit-wiseand message-wise UEPs(except the single message case for missed detection). The distinction between false-alarm and missed-detection formalizations for message-wise UEPis also considered. All results presented are at rates close to capacity. [J240]

"Transmission surveillance and self-restoration against fibre fault for time division multiplexing using passive optical network"

This study proposes a practical transmission surveillance and self-protection scheme for time division multiplexing using passive optical network (TDM-PON) with centralised monitoring and self-restorable apparatus. Troubleshooting a TDM-PON involves locating and identifying the source of an optical problem in what may be a complex optical network topology that includes several optical line terminals (OLTs), optical splitters, fibres and optical network units (ONUs). Since most components in the network are passive, a large part of the issues are due to dirty/damaged/misaligned connectors or breaks/macrobends in optical fibre cables. These will affect one, some or all subscribers in the network, depending on the location of the problems. The proposed scheme is able to prevent and detect the occurrence of fibre faults in a network system through centralised monitoring and remotely operate from a central office via Ethernet connection. Even with fibre fault prevention mechanisms, failures will still occur. Therefore fibre fault detection is required in order to detect potential faults and precisely localise the exact failure location. Whenever any failure occurs on the primary entity, the proposed system can protect and switch the failure line to the protection line to ensure that traffic flows continuously. Meanwhile, the failure information will be delivered to field engineers for taking appropriate recovery action to treat the fibre fault and failure link. One suggestion in point-to-multipoint (P2PM) applications has been proposed with the experimental results as the feasibility approach. This approach has bright prospects for improving the survivability and reliability as well as increasing the efficiency and monitoring capabilities in TDM-PON. [J241]

"Can Cognitive Science Help Us Make Online Risk More Tangible?"

Understanding the mental processes engaged by different representations of risk information is critical for the design of effective online risk communication. [J242]

"Data-centric security: Integrating data privacy and data security"

Classifying data according to its permissible use, appropriate handling, and business value is critical for data privacy and security protection. This is essential for compliance with the constantly evolving regulatory landscape concerning protected data. Problems arise when users compromise data privacy and security by overlooking the critical need to manage data according to these requirements. This paper considers the creation and application of data classification systems for security and privacy purposes. It focuses primarily on classifying information in a meaningful way through the use of a partially automated methodology that normalizes and classifies structured data throughout an enterprise. We introduce the three pillars of the data-centric security model, which are based on the data-centric security classification offering by IBM Global Business Services (GBS) and the IBM Research Division. In particular, we describe the data classification pillar of the data-centric security architecture, which provides the framework and method for partially automated classification of data to meet the demands of compliance standards. [J243]

"On the Vulnerabilities and Protections of the OLSR ad hoc Routing Protocol from the point of view of Trust"

The goal of this paper is to explicit the different types of trust relations between entities which exchange routing information and establish a routing infra-structure based on the OLSR protocol. One such entity assumes the other entities will behave in a particular way and the relations coming from this trust behavior are expressed in this paper using a formal language. This approach highlights the process of trust construction in OLSR and allows the analysis of trust requirements for this protocol, as well as the expression of attacks related to the betrayal of trust relations. This analysis allows the formal description of the reasoning for OLSR entities to have a protective mistrust behavior when acting based on trust relations. [J244]

"Bickering In-Depth: Rethinking the Composition of Competing Security Systems"

A vast array of security software exists, and because most of it addresses only relatively small facets of information security, it remains unclear how users should compose such software to achieve a reasonable degree of protection coverage. Furthermore, the many companies, organizations, and individuals that create such software don't design it to cooperate with similar software. We believe the resulting level of competition for resources and measurement points (kernel, library, or user hooks; disk access events; the system call API; and so on) can unnecessarily degrade system performance and interfere with the efficacy of the systems themselves. In essence, the broad call for "defense in-depth" can exacerbate existing performance and usability problems and lead to an unintentional loss of security. We suggest a paradigm in which security programmers intentionally design their code to cooperate with similar software by negotiating over security-critical resources, system measurement points, event types, and trusted information flow paths. [J245]

"Time-Domain Investigation on Cable-Induced Transient Coupling Into Metallic Enclosures"

A hybrid time-domain method is proposed for characterizing electromagnetic interference (EMI) signals coupled into some composite structures with metallic enclosures, braided shielded cable, printed circuit boards, and even lumped active devices. In order to rapidly capture the induced interior EMI, the finite-difference time-domain, modified node analysis, and multiconductor transmission lines methods are combined together and implemented successfully. Numerical investigation is carried out to demonstrate the frequency-dependent transfer impedance of the coaxial cable, the induced voltage at the place of active loaded element in the transmission line network, and the enclosure shielding effectiveness of these composite enclosures. The captured transient response information is useful for further designing electromagnetic protection of the inner circuits against the impact of voltage or current surge caused by nonintentional as well as intentional electromagnetic interference. [J246]

"Strategies for field testing medium voltage cables"

In power systems where failures and power outages are unacceptable, preventative maintenance activities must be a priority. This article attempts to clarify the issues involved in condition assessment of cable systems. It outlines the available test methods, reviews deterioration and failure mechanisms affecting the common cable types, provides simplified guidelines for deciding which tests will provide the best condition assessment information for each situation. The IEEE 400 standard might be the most widely used which provide information about field testing MV cables and components. [J247]

"Behavior Forensics With Side Information for Multimedia Fingerprinting Social Networks"

In multimedia social networks, there exists complicated dynamics among users who share and exchange multimedia content. Using multimedia fingerprinting as an example, this paper investigates the human behavior dynamics in the multimedia social networks with side information. Side information is the information other than the colluded multimedia content that can help increase the probability of detection. We study the impact of side information in multimedia fingerprinting and show that the statistical means of the detection statistics can help the fingerprint detector significantly improve the collusion resistance. We then investigate how to probe the side information and model the dynamics between the fingerprint detector and the colluders as a two-stage extensive game with perfect information. We model the colluder-detector behavior dynamics as a two-stage game and find the equilibrium of the colluder-detector game using backward induction and show that the min-max solution is a Nash equilibrium, which gives no incentive for everyone in the multimedia fingerprint social network to deviate. This paper demonstrates that the proposed side information can significantly help improve the system performance to almost the same as the optimal correlation-based detector. Such result opens up a new scope in the research of fingerprinting system that given any fingerprint code, leveraging side information can improve the collusion resistance. Also, we provide the solutions to how to reach optimal collusion strategy and the corresponding detection, thus lead to a better protection of the multimedia content. [J248]

"Detecting Code Alteration by Creating a Temporary Memory Bottleneck"

We develop a new technique whereby a poll worker can determine whether the software executing on electronic

voting machines on election day has been altered from its factory version. Our generalized approach allows a human, using a known challenge-response pair, to detect attacks that involve modification or replacement of software on a computer based on the time it takes the computer to provide a correct response to a challenge. We exploit the large difference between main memory access times and cache memory access or CPU clock cycle times to significantly increase the time required to compute the right response when the software has been changed. [J249]

"Interadministrative Challenges in Managing DNSKEYs"

Although the visible deployment of domain name system security extensions is growing at a tremendous rate, evidence suggests that managing cryptographic keys is deceptively complex. Here, the authors outline the problem of managing DNSKEYs and present a survey comparison of existing proposed solutions. [J250]

"Enhancing Electronic Voting Machines on the Example of Bingo Voting"

The main purpose of cryptographic voting schemes is to provide transparency while protecting ballot secrecy and to enable a fast tally. In this paper, we address three major issues of cryptographic voting schemes. First we discuss the problem of secrecy and coercion resistance in the situation of a corrupted voting machine. While hard to obtain in general, we propose and analyze a novel approach that uses encapsulated design and minimizes the information that can compromise ballot secrecy. The second issue we address is the assumption that an adversary does not know which receipts are checked and the problem of receipt stealing. Many voting schemes with receipts share this vulnerability. We provide a solution that increases protection of each vote and which can be generalized for voting schemes that use computers to form the receipt. The last issue discussed in this paper is the question of how an election can be contested. For this, an error or a manipulation must not only be detected but also proven. While the problems and solutions are described for Bingo Voting, we argue that the problems are shared by many cryptographic voting schemes and that the solutions presented in this work give insight in the prerequisites needed for a secure election. [J251]

"Probabilistic Versus Deterministic Algebraic Cryptanalysis-A Performance Comparison"

In this work, the performance of probabilistic algebraic attacks is compared to classical (fast) algebraic attacks in the context of their application to certain linear feedback shift register (LFSR)-based stream ciphers. Using some results from coding theory it is shown that in terms of time complexity classical deterministic algebraic attacks are in general a more efficient cryptanalytic tool, unless the filtering function F: GF (2)nrarr GF (2)mhas such a nonrandom structure that its cryptographic use is presumably refutable anyway. [J252]

"Security, Privacy, and the Role of Law"

US President Barack Obama promised a "new comprehensive approach" to cybersecurity and guaranteed to preserve "personal privacy and civil liberties," but the administration has stopped short of committing to the legal changes necessary to protect either information infrastructure or privacy. This tendency to undervalue law as a tool for enhancing both security and individual privacy is shared with other governments. Sound cybersecurity policy requires better incentives to secure data and systems, and those incentives will emerge, at least in part, from legal requirements. Similarly, serious efforts to protect against cyberthreats will compromise privacy and other civil rights unless those rights are protected by law. [J253]

"Incentives to Innovate: Improve the Past or Break with It?"

Does more expansive copyright law increase creativity by discouraging adaptations of existing work? The author discusses examples from cooking, boatbuilding, and the theater. [J254]

"New Models for Old"

When faced with a new thing, human beings do something very sensible. They try to harness previous experience and intuition in service of the new thing. How is this new thing like something that I already know and understand? Trying to model the new thing on some old thing can be efficient, making it easier to reason about the new thing by using analogies adopted from previous experience. We're in the midst of a huge society-wide change to move record keeping from paper systems to digital ones. In consequence, a vast number of existing rules can and should be rethought and revised. No better time than now, and no one better to do it than we. [J255]

"Think Piece: Preserving Records of the Past, Today"

I propose that as part of our research and writing responsibilities that we add another: to help create the materials that we and future historians will need, even if we are not rewarded or recognized for doing so. Specifically, I think we should agree to contribute the following to the greater community of historians. [J256]

"Biophysical mechanisms of modification of skin optical properties in the UV wavelength range with nanoparticles"

In this paper, by means of the Mie theory and Monte Carlo simulations we investigate modification of optical properties of the superficial layer of human skin (stratum corneum) for 310- and 400-nm ultraviolet (UV) radiation by embedding of 35-200-nm-sized particles of titanium dioxide (TiO2)and silicon (Si). Problem of skin protection against UV light is of major importance due to increased frequency of skin cancer provoked by excessive doses of accepted UV radiation. For 310-nm light, the optimal sizes of the TiO2and Si particles are found to be 62 and 55 nm, respectively, and for 400-nm radiation, 122and 70 nm, respectively. [J257]

"Mathematical Model for Low-Rate DoS Attacks Against Application Servers"

In recent years, variants of denial of service (DoS) attacks that use low-rate traffic have been proposed, including the Shrew attack, reduction of quality attacks, and low-rate DoS attacks against application servers (LoRDAS). All of these are flooding attacks that take advantage of vulnerability in the victims for reducing the rate of the traffic. Although their implications and impact have been comprehensively studied, mainly by means of simulation, there is a need for mathematical models by which the behaviour of these sometimes complex processes can be described. In this paper, we propose a mathematical model for the LoRDAS attack. This model allows us to evaluate its performance by relating it to the configuration parameters of the attack and the dynamics of network and victim. The model is validated by comparing the performance values given against those obtained from a simulated environment. In addition, some applicability issues for the model are contributed, together with interpretation guidelines to the model's behaviour. Finally, experience of the model enables us to make some recommendations for the challenging task of building defense techniques against this attack. [J258]

"Verification of Distributed Real-Time Computer Network Architecture Associated With Off-The-Shelf and Dedicated Technologies"

This paper introduces an architecture for computer communications applied to the operation and maintenance of power systems, the distributed real-time computer network architecture (DRNA). The architecture consists of four functional entities, namely, application programs associated with information models, an adaptation function, a transport function, and network- and security-management functions to achieve seamless, real-time, adaptive, and secure information exchange between distributed power system control devices. DRNA uses off-the-shelf and standardized technologies along with dedicated ones. Through careful application of the technology, an experimental setup of a distributed cooperative voltage-control network was constructed in a power system simulator to verify the architectural concept. The implemented technologies include mobile agents, middleware for prioritized and redundant communication schemes, label-switched and Ethernet-based transport networks, and a secure virtual private network. The experiment demonstrated the effectiveness of DRNA. [J259]

"Play the IT security game fun for all the enterprise!"

IT security is no game, and those who practice it can expect no respite from the onslaught of online threats except for this game. You have to steer your organisation past the hackers, script kiddies and disgruntled employees. Your future as CIO is at stake, and your decisions could spell the difference between winning or losing. All you need are a couple of standard games dice, and some form of place marker for each player e.g., a tiddly-wink. Start the game with three products or services you can buy that you think should enhance your security. As you move around the board, you find out whether or not they work. One piece of bad planning can send you back to the beginning. When you land on a Random Event, and you haven't implemented the necessary protection, you take the full impact. If you have, you get to laugh in the face of chance and roll again. Serpents of unforseen fate lurk elsewhere: green slithers you up, while red slithers you down. [J260]

"Accumulated-Downtime-Oriented Restoration Strategy With Service Differentiation in Survivable WDM Mesh Networks"

Telecommunications service providers (SP) should place survivability expectations by guaranteeing maximal allowed system downtime for service-level agreement (SLA)-differentiated services. Furthermore, SPs should continuously focus on utilizing network resources effectively, by considering the bounded network capacity and the growth of future data traffic. In order to improve different service availabilities and achieve high resource efficiency, we present a novel restoration scheme by jointly considering accumulated downtime and SLA

requirements of faulty connections. While most past related works have focused on providing statistical guarantees on availability when a connection is provisioned, our current approach recognizes that, after a connection has been in existence, it could be ldquoaheadrdquo (or ldquobehindrdquo) its performance guarantee based on what network outages it might have experienced, so the resources allocated to it may be revised judiciously. When a link failure occurs, two sets of faulty connections are examined: (a) connections whose primary or restoration path is disrupted by the failure and (b) connections that are in the ldquodownrdquo state due to some previous failures (which have not been repaired yet). An affected connection is switched to its pre-computed or an alternate restoration path if necessary, when its accumulated downtime plus the link repair time will exceed its SLA requirement. The scheme provides differentiated restoration to existing connections upon a link failure in order to satisfy the connectionspsila availability requirements. We also propose an upgraded version of the scheme that incorporates both excess capacity and resource preemption into the scheme. Given the network capacities and the current network state including routing information for all existing connections, a faulty connection is restored to its restoration path as long as there is enough excess capacity along the path. Otherwise, when protection switch- ing of a high-SLA connection fails due to limited bandwidth on some link(s), it preempts restoration capacity on each link from a low-SLA connection if both disrupted connections share the same restoration capacity and the availability requirement of the low-SLA connection is not violated. Finally, we report simulation results for a large carrier-scale network to show computational performance of our proposed algorithm. The results demonstrate that the algorithm achieves a high availability satisfaction rate and good resource utilization, as well as greatly reduces protection-switching overhead. [J261]

"Automobile security concerns"

Automotive theft and hijacking are traditionally the major automobile security concerns. The Federal Bureau of Investigation (FBI) Uniform Crime Reports (UCR) state that the number of automobiles stolen each year fluctuated around 1,200,000 from 1997 to 2006 (Figure 1), without having a steady trend. Common ways of stealing cars include carjacking, breaking windows or jimmying locks to gain entry, deactivating the alarm or steering wheel lock by cutting wires, deceiving manufacturers to make a replacement key by providing specific information of automobiles, or (most frequently) keys left in the automobile by their careless owners. Admittedly these threats are low tech. Well-known automotive security features, such as alarms, entry lock, and transmission or wheel lock, prevent the threats to some extent. [J262]

"Simplification of Packet-Symbol Decoding With Errors, Deletions, Misordering of Packets, and No Sequence Numbers"

In this paper, a new method is described which builds on Mitzenmacher's idea of adding a different pseudorandom number to each packet to help decode packet-symbol low-density codes, with deletions, errors, and out-of-order reception, without sequence numbers. The new method has lower decoding complexity than the original method. The most basic form of the new method applies to any parity-check code structure, but is limited to a rather small number of packets in the code. Decoding success is slightly inferior to an ideal erasure channel, which would require sequence numbering and error detection in each packet. Error detection is needed only for the whole code, amounting to usually less than one bit per packet symbol. Moreover, if error detection can resolve one of a small number of alternatives, the ordered case performs almost as well as the ideal erasure channel. Ways are shown to modify the basic algorithm for use with long codes, possibly approaching the erasure channel capacity limit. [J263]

"On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers"

In this paper, the complexity of applying a guess and determine attack to so-called Linear Feedback Shift register (LFSR)-based stream ciphers is analyzed. This family of stream ciphers uses a single or several LFSR and a filtering function F: GF(2)nrarr GF(2)mto generate the blocks of m ges 1 keystream bits at the time. In difference to a classical guess and determine attack, a method based on guessing certain bits in order to determine the remaining secret key/state bits, our approach efficiently takes advantage of the reduced preimage space for relatively large m and at the same time employing the design structure of the cipher. Several variations of the algorithm are derived to circumvent the sensitivity of attack to the input data, n, m and the key length. In certain cases, our attack outperforms classical algebraic attacks; these being considered as one of the most efficient cryptanalyst tools for this type of ciphers. A superior performance of our attack over algebraic attacks is demonstrated in case the filtering function belongs to the extended Maiorana-McFarland class. [J264]

"Linear diversity-embedding STBC: design issues and applications"

We design a novel class of space-time codes, called linear diversity-embedding space-time block codes (LDE-STBC) where a high-rate STBC is linearly superimposed on a high-diversity STBC without requiring channel

knowledge at the transmitter. In applying this scheme to multimedia wireless communications, each traffic type constitutes a transmission layer that operates at a suitable rate-diversity tradeoff point according to its quality-of-service requirements. This, in turn, provides an unequal-error-protection (UEP) capability to the different information traffic types and allows a form of wireless communications where the high-rate STBC opportunistically takes advantage of good channel realizations while the embedded high-diversity STBC ensures that at least part of the information is decoded reliably. We investigate transceiver design issues specific to LDE-STBC including reduced-complexity coherent decoding and effective schemes to vary the coding gain to further enhance UEP capabilities of the code. Furthermore, we investigate the application of LDE-STBC to wireless multicasting and demonstrate its performance advantage over conventional equal-error-protection STBC. [J265]

"Random-Coding Lower Bounds for the Error Exponent of Joint Quantization and Watermarking Systems"

We establish random-coding lower bounds to the error exponent of discrete and Gaussian joint quantization and private watermarking systems. In the discrete system, both the covertext and the attack channel are memoryless and have finite alphabets. In the Gaussian system, the covertext is memoryless Gaussian and the attack channel has additive memoryless Gaussian noise. In both cases, our bounds on the error exponent are positive in the interior of the achievable quantization and watermarking rate region. [J266]

"Digital Image Source Coder Forensics Via Intrinsic Fingerprints"

Recent development in multimedia processing and network technologies has facilitated the distribution and sharing of multimedia through networks, and increased the security demands of multimedia contents. Traditional image content protection schemes use extrinsic approaches, such as watermarking or fingerprinting. However, under many circumstances, extrinsic content protection is not possible. Therefore, there is great interest in developing forensic tools via intrinsic fingerprints to solve these problems. Source coding is a common step of natural image acquisition, so in this paper, we focus on the fundamental research on digital image source coder forensics via intrinsic fingerprints. First, we investigate the unique intrinsic fingerprint of many popular image source encoders, including transform-based coding (both discrete cosine transform and discrete wavelet transform based), subband coding, differential image coding, and also block processing as the traces of evidence. Based on the intrinsic fingerprint of image source encoders, we construct an image source coding forensic detector that identifies which source encoder is applied, what the coding parameters are along with confidence measures of the result. Our simulation results show that the proposed system provides trustworthy performance: for most test cases, the probability of detecting the correct source encoder is over 90%. [J267]

"Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens"

Information security and privacy on the internet are critical issues in our society. In this research, we examine factors that influence Internet users' private-information-sharing behavior. Based on a survey of 285 preteens and early teens, who are among the most vulnerable groups on the Web, this study provides a research framework that explains an internet user's information privacy protection behavior. According to our study results, internet users' information privacy behaviors are affected by two significant factors: (1) users' perceived importance of information privacy and (2) information privacy self-efficacy. The study also found that users believe in the value of online information privacy and that information privacy protection behavior varies by gender. Our findings indicate that educational opportunities regarding internet privacy and computer security as well as concerns from other reference groups (e.g., peer, teacher, and parents) play an important role in positively affecting the Internet users' protective behavior regarding online privacy. [J268]

"Compress-Forward Coding With BPSK Modulation for the Half-Duplex Gaussian Relay Channel"

This paper studies compress-forward (CF) coding with BPSK modulation for the half-duplex Gaussian relay channel. In CF relaying, Wyner-Ziv coding is applied at the relay to exploit the joint statistics between signals at the relay and the destination. We propose Slepian-Wolf coded nested scalar quantization (SWCNSQ) for practical Wyner-Ziv coding at the relay. We first provide the achievable rate of SWCNSQ based CF relaying as a performance benchmark, and then present a practical code design using low-density parity-check (LDPC) codes for error protection at the source, and nested scalar quantization plus irregular-repeat accumulation (IRA) codes for CF coding at the relay. The degree distributions of the LDPC and IRA codes are optimized using extrinsic information transfer charts and Gaussian approximation. Under discretized density evolution for asymptotically large block lengths, our optimized code design operates 0.11-0.21 dB away from the SWCNSQ limit for CF relaying. Simulations with LDPC/IRA codes of length 2 times 105bits show a performance gap of 0.27-0.38 dB from the achievable rate. [J269]

"Identification of Cross-Country Fault of Power Transformer for Fast Unblocking of Differential Protection"

Due to the different ratings of the current transformers (CT) located on different sides of power transformer, only the CT of low ratings will saturate when the power transformer experiences a heavy through fault, leading to false differential current. Such type of external fault can be identified from the internal one if the differential protection is equipped with the percentage restraint characteristic together with the method using operation time difference between pickup element and differential protection. However, the differential protection will be wrongly blocked as well if a cross-country fault occurs. According to the investigations in this paper, in the event of an external fault accompanied by the CT saturation, the variation of most samples of the secondary current of the saturated CT is inversely proportional to the variation of the differential current. Comparatively, this law cannot be followed on the occasion of an internal fault. In this case, the locus of the variation of the saturated secondary current with the differential current can be used to dynamically discriminate if an external fault develops to an internal fault. With the method proposed in this paper, the ability of the differential protection immune to cross-country fault can be improved further. The effectiveness of the proposed method is verified with the simulation tests. [J270]

"Secure Cyberspace: Answering the Call for Intelligent Action"

As information technology permeates all societal layers and its use crosses increasingly national boundaries, information security has become of paramount importance. Understanding what motivates information security is part of the hard work in planning the mechanisms that will assure it. Arguably, ubiquitous networking—for a wide range of personal, commerce, enterprise, and national purposes—is responsible for many recent productivity gains. But with this convenience has come vulnerability to those who seek to do damage or benefit illegally. Today's dynamic technology marketplace—with product generations now measured in months—gives increased choice of functionality and style to millions of potential buyers and their escalating expectations. However, with every new device comes at least some segment of the user population that doesn't understand new functionality and, consequently, experiences decreased reliability and reduced privacy. [J271]

"Enabling secure service discovery in mobile healthcare enterprise networks"

Advances in wireless networks, sensors, and portable devices offer unique chances to deliver novel anytime anywhere medical services and information, thus enabling a wide range of healthcare applications, from mobile telemedicine to remote patient monitoring, from location-based medical services to emergency response. Mobile e-health has great potential to extend enterprise hospital services beyond traditional boundaries, but faces many organizational and technological challenges. In pervasive healthcare environments, characterized by user/service mobility, device heterogeneity, and wide deployment scale, a crucial issue is to discover available healthcare services taking into account the dynamic operational and environmental context of patient-healthcare operator interactions. In particular, novel discovery solutions should support interoperability in healthcare service descriptions and ensure security during the discovery process by making services discoverable by authorized users only. This article proposes a semantic-based secure discovery framework for mobile healthcare enterprise networks that exploits semantic metadata (profiles and policies) to allow flexible and secure service search/retrieval. As a key feature, our approach integrates access control functionalities within the discovery framework to provide users with filtered views on available services based on service access requirements and user security credentials. [J272]

"Regular Simplex Fingerprints and Their Optimality Properties"

This paper addresses the design of additive fingerprints that are maximally resilient against linear collusion attacks on a focused correlation detector, as defined below. Let Nbe the length of the host vector and Mles N+ 1 the number of users. The focused detector performs a correlation test in order to decide whether a user of interest is among the colluders. Both the fingerprint embedder and the colluders are subject to squared-error distortion constraints. We show that simplex fingerprints maximize a geometric figure of merit for this detector. In that sense they outperform orthogonal fingerprints but the advantage vanishes as Mrarr infin. They are also optimal in terms of minimizing the probability of error of the focused detector when the attack is a uniform averaging of the marked copies followed by the addition of white Gaussian noise. Reliable detection is guaranteed provided that the number of colluders KLt radic(N). Moreover, we study the probability of error performance of simplex fingerprints for the focused correlation detector when the colluders use nonuniform averaging plus white Gaussian noise attacks. [J273]

"When Sensitive IT Information Crosses Borders"

The seizure of information-bearing devices at the US border generates ethical challenges for organizations and their employees as well as government agencies and their employees. Organizations and government agencies can reduce the problems associated with these seizures by following specific policies and procedures. On one hand, agencies enforcing policies that might involve legal but proprietary information should be open about their policies and their effectiveness, but on the other, organizations should take care to protect their sensitive information and to not put their employees in difficult no-win situations when traveling outside the country. [J274]

"A SWIFT Take on Identity Management"

A proposed identity management framework provides privacy protection, by means of virtual identities, and cross-layer single sign-on for users who subscribe to multiple service and identity providers. [J275]

"Privacy and/or Security: Take Your Pick"

The concepts of privacy and security are distinct, but they're often considered synonymously when applied to computational systems. This article explores the conceptual differences between computational privacy and security and suggests four mutually exclusive models that define four different fundamental approaches to privacy and security during design. It's crucial that developers make a conscious and explicit decision how the two concepts should be approached early during system design. [J276]

"The Reaction Time to Web Site Defacements"

Web site defacement has become a common threat for organizations exposed on the Web. Several statistics indicate the occurrence rate of these incidents but not how long these defacements typically last. The authors present the results of a two-month study of more than 62,000 defacements to determine whether and when a reaction to a defacement occurs. Such reaction times tend to be unacceptably long-often several days-and with a long-tailed distribution. [J277]

"On the Current Peak Estimates Provided by Lightning Detection Networks for Lightning Return Strokes to Tall Towers"

The peak current estimation of lightning detection networks for strikes to tall towers is discussed in this paper. Such systems are sometimes calibrated using return-stroke current data obtained by means of rocket-triggered lightning or instrumented towers of relatively short height. However, for strikes to electrically tall towers, they tend to overestimate the return-stroke current peak. In this case, in fact, the associated radiated electromagnetic fields, from which the return-stroke current is estimated, experience a significant enhancement with respect to the field that would be radiated if the same return stroke was initiated at ground level or on a short tower. Two approaches to correct the current estimates of a lightning detection network for a lightning strike to a tall tower are discussed and applied to the current measurements obtained at the CN Tower in Toronto in the summer of 2005, for which estimates were available from the North American Lightning Detection Network (NALDN). It is shown that correcting the NALDN estimates using the so-called tower factor obtained from theoretical studies results in an excellent estimation of lightning current peaks. [J278]

"Effects of Outdated Control Information in Control-Plane-Enabled Optical Networks With Path Protection"

New signaling suites for a distributed control plane in wavelength division multiplexing (WDM) networks, such as generalized multiprotocol label switching (GMPLS) and automatic switched optical networks (ASON), allow one to cope with the increasing variability of traffic patterns to be supported by operators by providing a means to dynamically set up and release connections. The dissemination of link-state information [usually provided by routing protocols such as open-shortest-path-first traffic engineering (OSPF-TE)] is essential in this kind of control-plane enabled network: in particular, this information has to be continuously updated to allow routing algorithms to efficiently carry out the path computation. Most of the studies on dynamic traffic routing tend to neglect the effect of delays in control-information distribution on routing performance: in particular, even when the control plane is considered as in testbeds, emulators, or some simulations, the analysis of the effects of control plane delays is limited to a small range of values, applicable to well-specified contexts. Applying a very general control-delay representation, we are able to provide a wide-range simulative study to quantify the effect of signaling on routing performance, mainly by using the blocking probability metric. We are able to evaluate the effect of outdated information (1) for a wide interval of control delay values, (2) for a large set of routing scenarios, considering, e.g., unprotected, dedicated, and shared path protection routing, and (3) quantifying the different delay effects in the absence or in the presence of wavelength conversion capabilities. [J279]

"Content sharing between home networks by using personal information and associated fuzzy vault scheme"

Content sharing is getting popular in home network as well as in social media. Content sharing inside home is usually done among family members, while that between different home networks is done by friends and even anonymous users. Especially, anonymous users could access contents in home networks which could act like home portals. To protect content in home servers, the contents can be encrypted by key and the key can be shared among users. However it is quite challenging to distribute the key to anonymous users. In this paper, we present a method for sharing contents securely among different home networks. We propose a method of content sharing between anonymous users, who have similar personal preferences about the contents. The personal preferences include user profiles and contents preference. With the proposed method, a content sharing community is created for content delivery between different home networks. The community allows content creators to deliver contents to other users, who have similar personal information and can consume the contents without any leakage of personal information. In order to verify the usefulness of the proposed method, experiments were performed. The results showed that contents in one home server were securely shared with users of the other home server, if both have similar personal information. [J280]

"Online Partitioning for Scalable and Survivable Optical Networks"

Given the trend of rapid growth, the manageability and survivability of future optical networks, even for a single administrative domain, are imminent challenges. For a large-scale mesh network with dynamic traffic, maintaining the global state information in a centralized fashion is impractical. Hence, distributed schemes are needed to organize nodes and to manage state information in a more localized manner. One such scheme for organizing nodes is to logically partition or cluster the nodes into a hierarchical structure. However, in optical networks, physically disjoint routes are sought for failure-protection purposes, where the working path and the backup path of a request traverse diverse shared risk link groups (SRLGs). Hence, the clustering of nodes should also be effective in yielding SRLG diversity. In this paper, we address the problem of determining the appropriate clustering of nodes for a large wavelength division multiplexed (WDM) network. We suggest an easy-to-implement, dynamic, and distributed technique that forms clusters adaptively in response to the current network conditions, e.g., node connectivity, bandwidth availability (or traffic load), and SRLGs. We find that considering risk group sharing in network partitioning best handles both scalability and survivability. Simulation results verify the viability of the proposed approach. [J281]

"Diagnosis of Broken-Bar Fault in Induction Machines Using Discrete Wavelet Transform Without Slip Estimation"

The aim of this paper is to present a wavelet-based method for broken-bar detection in squirrel-cage induction machines. The frequency-domain methods, which are commonly used, need speed information or accurate slip estimation for frequency-component localization in any spectrum. Nevertheless, the fault frequency bandwidth can be well defined for any squirrel-cage induction machine due to numerous previous investigations. The proposed approach consists in the energy evaluation of a known bandwidth with time-scale analysis using the discrete wavelet transform. This new technique has been applied to the stator-current space-vector magnitude and the instantaneous magnitude of the stator-current signal for different broken-bar fault severities and load levels. [J282]

"Phase of Target Scattering for Wetland Characterization Using Polarimetric C-Band SAR"

Wetlands continue to be under threat, and there is a major need for mapping and monitoring wetlands for better management and protection of these sensitive areas. Only a few studies have been published on wetland characterization using polarimetric synthetic aperture radars (SARs). The most successful results have been obtained using the phase difference between HH and VV polarizations, phiHH- phiVV, which has shown promise for separating flooded wetland classes. Recently, we have introduced a new decomposition, the Touzi decomposition, which describes target scattering type in terms of a complex entity, the symmetric scattering type. Huynen's target helicity is used to assess the symmetric nature of target scattering. In this paper, the new complex-scattering-type parameters, the magnitude alphasand phase Phialphas, are investigated for wetland characterization. The use of the dominant-scattering-type phase Phialphasmakes it possible to discriminate shrub bogs from poor (sedge or shrub) fens. These two classes cannot be separated using phiHH- phiVV, or the radiometric scattering information provided by alphas, the Cloude alpha, the entropy H, and the multipolarization HH-HV-VV channels. phialphas, which cannot detect deep (45 cm below the peat surface) water flow in a bog, is more sensitive to the shallower (10-20-cm) fen beneath water, and this makes possible the separation of poor fens from shrub bogs. Phialphasalso permits the discrimination of conifer-dominated treed bog from upland deciduous forest under leafy conditions. Target helicity information is exploited to introduce a new parameter, the target asymmetry. The latter is shown very promising for detection of forest changes between leafy and no-leaf

conditions. The analysis of low-entropy marsh scattering showed that both the scattering-type magnitude and phas--e alphasand Phialphas, respectively, as well as the maximum polarization intensity of the dominant scattering m, are needed for a better understanding of marsh complex scattering mechanisms. The unique information provided by the new roll-invariant decomposition parameters are demonstrated using repeat-pass Convair-580 polarimetric C-band SAR data collected in June and October 1995 over the RAMSAR Mer Bleue wetland site near Ottawa (Canada). [J283]

"On the primary exclusive region of cognitive networks"

We study a cognitive network consisting of a single primary transmitter and multiple secondary, or cognitive, users. The primary transmitter, located at the center of the network, communicates with primary receivers within a disc called the primary exclusive region (PER). Inside the PER, no cognitive users may transmit, in order to guarantee an outage probability for the primary receivers within. Outside the PER, uniformly distributed cognitive users may transmit, provided they are at a certain protected radius from a primary receiver. We analyze the aggregated interference from the cognitive transmitters to a primary receiver within the PER. Based on this interference and the outage guarantee, we derive bounds on the radius of the PER, showing its interdependence on the receiver protected distance and other system parameters. We also extend the analysis to allowing the cognitive users to scale their power according to the distance from the primary transmitter. These studies provide a closed-form, theoretical analysis of such a network geometry with PER, which may be relevant in the upcoming spectrum sharing actions. [J284]

"Performance of convolutional codes in asynchronous CDMA communications under imperfect phase-tracking conditions"

In this paper, the performance of short constraint length convolutional codes in imperfect phase tracking conditions is discussed. Convolutional codes are used to provide error protection to a particular user in an Asynchronous CDMA (A- CDMA) system undergoing slow Rician fading. Maximum likelihood decoding with a Viterbi algorithm recovers the information symbols. A Phase Locked Loop (PLL) depicting the variations in the phase error for abrupt phase changes in the input signal is considered. Analytical bounds, which are useful in predicting the performance of the A-CDMA system are derived and plotted for the cases of infinite and finite channel memory. The upper bounds on the unconditional Bit Error Rate (BER) with Viterbi decoding are derived and plotted for the various convolutional codes considered. The simulated BERs are found to agree well with their upper bounds. [J285]

"A DC Signal Injection-Based Thermal Protection Scheme for Soft-Starter-Connected Induction Motors"

This paper proposes a remote and sensorless thermal protection scheme for soft-starter-connected induction motors. A dc signal injection-based method is used to estimate the stator winding resistance and, thus, the stator winding temperature. Based on continuous monitoring of the stator winding temperature, a thermal condition monitoring and protection scheme is proposed using only the motor's input voltages, currents, motor nameplate information, and the ambient temperature. An adaptive Kalman filter is designed to reduce the stator winding temperature estimation error. In addition, the influence of the cable resistance was investigated, and a compensation method is suggested to improve the accuracy of the estimated temperature. The requirements of the data acquisition system, such as sampling frequency and analog-to-digital conversion resolution, and their affects on the accuracy of the estimated temperature are also discussed in detail. The proposed thermal monitoring scheme has been validated from the experimental results of a 7.5-hp TEFC induction motor under various load conditions. The importance of this new thermal monitoring scheme lies in its remote and sensorless nature. [J286]

"Fingerprinting Compressed Multimedia Signals"

Digital fingerprinting is a technique to deter unauthorized redistribution of multimedia content by embedding a unique identifying signal in each legally distributed copy. The embedded fingerprint can later be extracted and used to trace the originator of an unauthorized copy. A group of users may collude and attempt to create a version of the content that cannot be traced back to any of them. As multimedia data is commonly stored in compressed form, this paper addresses the problem of fingerprinting compressed signals. Analysis is carried out to show that due to the quantized nature of the host signal and the embedded fingerprint, directly extending traditional fingerprinting techniques for uncompressed signals to the compressed case leads to low collusion resistance. To overcome this problem and improve the collusion resistance, a new technique for fingerprinting compressed signals called Anti-Collusion Dither (ACD) is proposed, whereby a random dither signal is added to the compressed host before embedding so as to make the effective host signal appear more continuous. The

proposed technique is shown to reduce the accuracy with which attackers can estimate the host signal, and from an information theoretic perspective, the proposed ACD technique increases the maximum number of users that can be supported by the fingerprinting system under a given attack. Both analytical and experimental studies confirm that the proposed technique increases the probability of identifying a guilty user and can approximately quadruple the collusion resistance compared to conventional Gaussian fingerprinting. [J287]

"Increasing Safety of Bomb Disposal Missions: A Body Sensor Network Approach"

During manned bomb disposal missions, the combination of the protective suit's weight (37 kg), physical activity, high ambient temperatures, and restricted airflow can cause the operative's temperature to rise to dangerous levels during missions, impairing their physical and mental ability. This work proposes to use body sensor networks (BSNs) to increase the safety of operatives in such missions through detailed physiological monitoring, fusion of health information, and remote alerts. Previous trials conducted by the authors have shown no correlation between the suit wearer's temperature at any single skin site and their core temperature, nor between single-point temperature variations and subjective thermal sensation. This paper reports on the development of a wearable, wireless, networked sensing system suitable for integration within the suit and deployment in manned missions. A sensor fusion and modeling approach is proposed that estimates the overall thermal sensation of the suit wearer, in real time, based on the multipoint temperature data. Zhang's thermal sensation model was used in this work. Modeling is performed locally to enable cooling system actuation, provide local feedback, and accommodate application specific constraints. Experimentation with the prototype confirms the importance of multisite skin measurement, timely cooling actuation, and monitoring the operative's thermal state. Evaluation of Zhang's model highlights the need for a bespoke model to account for suit and mission specific factors. The deployed BSN has been evaluated through experimental trials using a number of subjects in mission-like conditions and has been shown to be appropriate for the target application. [J288]

"Achievements in power [JHistory]"

The IEEE milestones in Electrical Engineering and Computing program is one of the most important responsibilities of the IEEE History Committee. Administered through the IEEE History Center, the program recognizes and honors technological innovation and excellence in the many fields of interest of IEEE. The principal purpose of the program is to promote public and scientific community awareness, knowledge, and understanding of the importance and rich history of electrotechnology. The program also publicizes significant engineering achievements in the locales where they occurred and helps to protect and preserve historically important information, artifacts, and sites. To be considered for milestone status, an achievement has to be at least 25 years old, involve a unique solution to an engineering problem, and have had regional or broader impact. [J289]

"Security through Information Risk Management"

Managing information risk means building risk analysis into every business decision. Chief information security officers widely agree that action plans must include risk categorization, communication, and measurement. [J290]

"Access Control Model Formalism using Adaptive Automaton"

Privacy is an important aspect when modeling computer systems which need to establish relationships among users and their information. To face this issue, many privacy protection mechanisms have been considered. Generic mechanisms deal with the information security of a certain user restricting a system in a way to have only relationships among subjects and objects which comply with this system rules. This paper presents an access control model formalism using adaptive automaton on a auditable privacy system. The adaptive automaton is suitable for this purpose, because of the self-modifications capacity and complex languages recognition. The model using the the proposed formalism is a new approach to privacy protection mechanisms, and is generic enough to be used not just in privacy, but in another classes of problems. [J291]

"Method for AC Powerline Impedance Measurement"

Methods exist today to estimate the AC powerline impedance by taking into account the various components in the distribution system. These calculations are fraught with error due to inaccurate electrical documentation and a lack of information about the physical construction of the system. However, the accuracy of these results is critical because they feed into the calculation of available energy for establishing the degree of arc flash hazard present at a location. This paper presents a novel method for determining the AC powerline resistance and inductance through a process of measuring the real-time reaction of the line to the controlled application of two known impedances. This method has been realized and tested to accurately measure powerline impedances as

high as 84 kA in 480-V motor control centers. The available energy can be calculated from this impedance to assist in the determination of the appropriate equipment necessary for arc flash protection. [J292]

"On the Assumption of Equal Contributions in Fingerprinting"

With a digital fingerprinting scheme, a vendor of digital copies of copyrighted material marks each individual copy with a unique fingerprint. If an illegal copy appears, it can be traced back to one or more guilty pirates due to this fingerprint. A coalition of pirates may combine their copies to produce an unauthorized copy with a false, hybrid fingerprint. It is often assumed in the literature that the members of the collusion will make equal contributions to the hybrid fingerprint, because nobody will accept an increased risk of being caught. We argue that no such assumption is valid apriori, and we show that a published solution by Sebe and Domingo-Ferrer can be broken by breaking the assumption. [J293]

"Asymptotic tradeoff between cross-layer goodput gain and outage diversity in OFDMA systems with slow fading and delayed CSIT"

There are two important aspects of cross-layer gains in multiuser OFDMA systems with slow fading channels. They are the system goodput gain as well as the packet diversity gain. The former aspect of cross-layer designs has been well- studied under perfect CSIT conditions and is known as the multi-user diversity gain (MuDiv). In cross-layer OFDMA systems with perfect CSIT, it is well known that the system throughput (ergodic capacity) scales in the order of O(log log Kldquo) due to the MuDiv gain, where K is the number users. However, in slow fading channels with delayed CSIT, there will always be potential packet errors (due to channel outage if the scheduled data rate exceeds the instantaneous mutual information) even if very strong channel coding is applied at the base station. In this case, the cross-layer packet outage diversity is important to protect the packet errors due to channel outage and there is a natural tradeoff between the goodput gain and packet diversity. In this paper, we shall focus on the asymptotic tradeoff analysis between the system goodput gain and the packet outage diversity gain in cross-layer OFDMA systems with delayed CSIT. [J294]

"Sustainable land use using consensus mapping and conflict resolution"

Land use conflicts are the typical example of spatial conflicts. They are intrinsically complex and require a comprehensive approach to their solutions. It is necessary to come to grips with the nature of their complexity to provide adequate support to deal with them. Development of land management plans through the participation of stakeholders is being appreciated and accepted as a requirement for sustainable land use. However, the involvement of stakeholders (participatory approach) gives rise to many questions. Who are the stakeholders? How to identify them? How to empower them? How to lead them through the process of negotiation? How to collate their interests to resolve the conflicts? How to facilitate this process? etc. This is an endeavour to answer the questions relevant to the support and facility that can be provided for conflict resolution by using the suitable techniques and technology. This paper introduces the concept of GIS-based collaborative decision-making and presents a general model that is developed on the basis of decision theory to support the process of conflict resolution in the context of sustainable land use. [J295]

"Silver Bullet Security Podcast Series"

{no data available} [J296]

"CROWN-C: A High-Assurance Service-Oriented Grid Middleware System"

A proposed grid middleware system includes specific enhancements to support the development and assessment of highly secure, dependable, service-oriented grid systems and applications. Service-oriented architectures can be defined as application architectures "within which all functions are defined as independent services. [J297]

"Cybersecurity Strategies: The QuERIES Methodology"

QuERIES offers a novel multidisciplinary approach to quantifying risk associated with security technologies resulting in investment-efficient cybersecurity strategies. R esearchers can use the QuERIES methodology to rigorously determine, for the first time, appropriate investment levels and strategies for the protection of intellectual property in complex systems. As a result, it can have a significant and immediate impact on the protection of critical IP, including weapons systems and chip designs, complex computer software, and databases containing personal and financial information. In this paper, initial testing of QuERIES in small-scale, realistic scenarios, were performed with results that suggest the methodology can significantly improve risk assessments in complex systems under attack by rational and capable adversaries. Such systems include

software, hardware, and data critical to national security and industrial competitiveness. Consequently, it is believed that QuERIES has wide applicability within both the DoD and private sectors. [J298]

"A Conceptual Framework for Assessing the Benefits of a Global Earth Observation System of Systems"

The aim of the Global Earth Observation System-of-Systems (GEOSS) is to improve the information available to decision makers, at all levels, relating to human health and safety, protection of the global environment, the reduction of losses from natural disasters, and achieving sustainable development. Specifically, GEOSS proposes that better international cooperation in the collection, interpretation, and sharing of Earth observation information is an important and cost-effective mechanism for achieving this aim. While there is a widespread intuition that this proposition is correct, at some point the following question needs to be answered: how much additional investment in Earth observation (and specifically, in its international integration) is enough? This leads directly to some challenging subsidiary questions, such as how can the benefits of Earth observation be assessed? What are the incremental costs of GEOSS? Are there societal benefit areas where the return on investment is higher than in others? The Geo-Bene Project has developed a ldquobenefit chainrdquo concept as a framework for addressing these questions. The basic idea is that an incremental improvement in the observing system (including its data collection, interpretation and information-sharing aspects) will result in an improvement in the quality of decisions based on that information. In turn, this will lead to better societal outcomes, which have a value. This incremental value must be judged against the incremental cost of the improved observation system. Since in many cases there will be large uncertainties in the estimation of both the costs and the benefits, and it may not be possible to express them in comparable monetary terms, we show how order-of-magnitude approaches and a qualitative understanding of the shape of the cost and benefit curves can help guide rational investment decisions in Earth Observation Systems. [J299]

"A RED-FEC Mechanism for Video Transmission Over WLANs"

This paper proposes a Random Early Detection Forward Error Correction (RED-FEC) mechanism to improve the quality of video delivered over Wireless Local Area Networks (WLANs). In contrast to previous FEC schemes, in which the rate determination information is fed back from the receiver side, in our proposed method, the redundancy rate is calculated directly at the wireless Access Point (AP) in accordance with the network traffic load, as indicated by the AP queue length. An analytical model is developed to predict the effective packet loss rate of a video stream delivered over a WLAN with RED-FEC protection. The numerical results show that the proposed RED-FEC mechanism consistently achieves higher recovery efficiency than a conventional FEC scheme under high and low network loading conditions. [J300]

"MAC layer misbehavior in wireless networks: challenges and solutions"

IEEE 802.11 CSMA/CA has been widely deployed as the primary MAC protocol for ad hoc networks and wireless LANs. It was designed with the assumption that nodes would follow proper operation of the protocol. Nodes, however, may choose to deviate in order to either obtain an unfair share of the available bandwidth or disrupt the services of the network. Accordingly, a misbehavior rooted at the MAC layer can be classified as selfish or malicious behavior. This article surveys the research activities related to MAC layer misbehavior; based on the operating principles and the objective of misbehaving nodes, we classify MAC layer misbehavior and present descriptions for each solution. We conclude with a brief summary of the key ideas and a general direction for future work. [J301]

"Determination of Optimal Distortion-Based Protection in Progressive Image Transmission: A Heuristic Approach"

In this paper, we describe a method for fast determination of distortion-based optimal unequal error protection (UEP) of bitstreams generated by embedded image coders and transmitted over memoryless noisy channels. The UEP problem is reduced to the more general problem of finding a path in a graph, where each path of the graph represents a possible protection policy, with the objective of selecting the best path being that one inducing minimal distortion. The problem is combinatorially complex and excludes a brute force approach. The solution is provided by applying heuristic information from the problem domain to reduce search complexity. In particular, we use graph search procedure suggested by Hart, well known in the field of artificial intelligence, to avoid exhaustive search. Numerical results show that this technique outperforms the method presented by Hamzaoui, in terms of mean square error (MSE) distortion and computational complexity. After testing our solution using analytical models of the operational distortion curves proposed by Charfi, we implement a transmission architecture that, using the actual distortion values generated by a real embedded coder, computes the optimal protection policy for the considered image, protects the packets, and transmits them over a channel.

[J302]

"A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System"

Cryptographic systems have been widely used in many information security applications. One main challenge that these systems have faced has been how to protect private keys from attackers. Recently, biometric cryptosystems have been introduced as a reliable way of concealing private keys by using biometric data. A fuzzy vault refers to a biometric cryptosystem that can be used to effectively protect private keys and to release them only when legitimate users enter their biometric data. In biometric systems, a critical problem is storing biometric templates in a database. However, fuzzy vault systems do not need to directly store these templates since they are combined with private keys by using cryptography. Previous fuzzy vault systems were designed by using fingerprint, face, and so on. However, there has been no attempt to implement a fuzzy vault system that used an iris. In biometric applications, it is widely known that an iris can discriminate between persons better than other biometric modalities. In this paper, we propose a reliable fuzzy vault system based on local iris features. We extracted multiple iris features from multiple local regions in a given iris image, and the exact values of the unordered set were then produced using the clustering method. To align the iris templates with the new input iris data, a shift-matching technique was applied. Experimental results showed that 128-bit private keys were securely and robustly generated by using any given iris data without requiring prealignment. [J303]

"Progress of the ITER equatorial vis/IR wide angle viewing system optical design"

The equatorial vis/IR wide angle viewing system is present in four ITER diagnostic equatorial ports. This instrument will cover a large field of view with high spatial and temporal resolutions, to provide real time temperature measurements of plasma facing components, spectral data in the visible range, information on runaway electrons, and pellet tracking. This diagnostic needs to be reliable, precise, and long lasting. Its design is driven by both the tokamak severe environment and the high performances required for machine protection. The preliminary design phase is ongoing. Paramount issues are being tackled, relative to wide spectral band optical design, material choice, and optomechanical difficulties due to the limited space available for this instrument in the ports, since many other diagnostics and services are also present. Recent progress of the diagnostic optical design and status of associated R&D are presented. [J304]

"ArchiSafe: Legally Compliant Electronic Storage"

Traditional data backup and storage processes have targeted speed, efficiency, and disaster recovery. Various governmental regulations now impose additional requirements that demand sophisticated archival management, including the ability to preserve documents' long-term authenticity and availability. [J305]

"E-Discovery: Identifying and Mitigating Security Risks during Litigation"

When producing electronically stored information (ESI) in response to lawsuits, businesses face several security risks as well as legal requirements they must satisfy. Customized document management programs and e-discovery policies are key tools in protecting against inadvertent disclosure as well as meeting business and legal needs. [J306]

"Phenomena of leaking electromagnetic waves and high frequency surges from isolated joint of gas insulated switchgear"

High frequency surges leaking through the insulated joint of a GIS were measured, using a model GIS, and the phenomena, characteristics and mechanism were clarified based on the experiment and the circuit theory. High frequency surges decrease the impedance of the insulated joint, producing an almost short circuit state, and the coefficient for refraction from the inside of the GIS tank to the grounding system becomes significantly small. In a multi-phase GIS, surges leaking through the insulated joint form the tank-to-tank mode voltage for the different phase tank, generating the voltage equal to the potential of the voltage application tank to ground. On the other hand, no potential to ground is directly generated to the adjoining bus. The amplitude and the frequency of surges leaking through the insulated joint of a GIS bus are almost identical to those calculated from the distributed constant circuit theory. The phenomena can be, therefore, reproduced using the EMTP through the simulation of the line part by the multi-phase distributed constant and the simulation of the insulated joint by the capacitance. [J307]

"Lookup-Table-Based Secure Client-Side Embedding for Spread-Spectrum Watermarks"

Today, mass-scale electronic content distribution systems embed forensic tracking watermarks primarily at the distribution server. For limiting the bandwidth usage and server complexity and enhancing scalability, it is

preferable to embed the watermark at the client. Embedding in these untrusted clients requires secure embedding methods that do not leak unmarked content or the watermarking secrets. In this work, we propose a secure watermark embedding scheme based on lookup tables for spread-spectrum watermarks, which are robust to noise and can be detected without comparison to the original content. We also develop fast detection mechanisms that make the watermark detection feasible for tracking systems with a large number of clients. Our fast detection algorithm improves detection speed of existing methods by six orders of magnitude in a typical system with millions of clients. [J308]

"Transactional Confidentiality in Sensor Networks"

In a sensor network environment, elements such as message rate, message size, mote frequency, and message routing can reveal transactional data-that is, information about the sensors deployed, frequency of events monitored, network topology, parties deploying the network, and location of subjects and objects moving through the networked space. Whereas the confidentiality of network communications content is secured through encryption and authentication techniques, the ability of network outsiders and insiders to observe transactional data can also compromise network confidentiality. Four types of transactional data are typically observable in sensor networks. Measures to limit the availability and utility of transactional data are essential to preserving confidentiality in sensor networks. [J309]

"Wireless Information-Theoretic Security"

This paper considers the transmission of confidential data over wireless channels. Based on an information-theoretic formulation of the problem, in which two legitimates partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the important role of fading is characterized in terms of average secure communication rates and outage probability. Based on the insights from this analysis, a practical secure communication protocol is developed, which uses a four-step procedure to ensure wireless information-theoretic security: (i) common randomness via opportunistic transmission, (ii) message reconciliation, (iii) common key generation via privacy amplification, and (iv) message protection with a secret key. A reconciliation procedure based on multilevel coding and optimized low-density parity-check (LDPC) codes is introduced, which allows to achieve communication rates close to the fundamental security limits in several relevant instances. Finally, a set of metrics for assessing average secure key generation rates is established, and it is shown that the protocol is effective in secure key renewal-even in the presence of imperfect channel state information. [J310]

"On the Fingerprinting Capacity Under the Marking Assumption"

We address the maximum attainable rate of fingerprinting codes under the marking assumption, studying lower and upper bounds on the value of the rate for various sizes of the attacker coalition. Lower bounds are obtained by considering typical coalitions, which represents a new idea in the area of fingerprinting and enables us to improve the previously known lower bounds for coalitions of size two and three. For upper bounds, the fingerprinting problem is modeled as a communications problem. It is shown that the maximum code rate is bounded above by the capacity of a certain class of channels, which are similar to the multiple-access channel (MAC). Converse coding theorems proved in the paper provide new upper bounds on fingerprinting capacity. It is proved that capacity for fingerprinting against coalitions of size two and three over the binary alphabet satisfies and, respectively. For coalitions of an arbitrary fixed size, we derive an upper bound on fingerprinting capacity in the binary case. Finally, for general alphabets, we establish upper bounds on the fingerprinting capacity involving only single-letter mutual information quantities. [J311]

"Need to Share vs. Need to Assure"

As a society, we have a tendency to send just about anything electronically these days. From business and personal information to pictures, jokes, and links to Web sites, we assume that the information we send is protected and will be delivered accurately to only the intended recipients. Although we might have corporate policies or personal guidelines about what information is posted, shared, and archived electronically, what is preached is often very different from what we practice. As the age of electronics and information sharing continues to grow, IT managers and the general public need to stop and think about what we need and want to share. [J312]

"Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards"

User authentication and key agreement is an important security primitive for creating a securely distributed information system. Additionally, user authentication and key agreement is very useful for providing identity privacy to users. In this paper, we propose a robust and efficient user authentication and key agreement scheme

using smart cards. The main merits include the following: 1) the computation and communication cost is very low; 2) there is no need for any password or verification table in the server; 3) a user can freely choose and change his own password; 4) it is a nonce-based scheme that does not have a serious time-synchronization problem; 5) servers and users can authenticate each other; 6) the server can revoke a lost card and issue a new card for a user without changing his identity; 7) the privacy of users can be protected; 8) it generates a session key agreed upon by the user and the server; and 9) it can prevent the offline dictionary attack even if the secret information stored in a smart card is compromised. [J313]

"Diversity Embedded Codes: Theory and Practice"

Diversity embedded codes are high-rate space-time codes that have a high-diversity code embedded within them. They allow a form of communication where the high-rate code opportunistically takes advantage of good channel realizations while the embedded high-diversity code provides guarantees that at least part of the information is received reliably. Over the past few years, code designs and fundamental limits of performance for such codes have been developed. In this paper, we review these ideas by giving the developments in a unified framework. In particular, we present both the coding technique as well as information-theoretic bounds in the context of Intersymbol Interference (ISI) channels. We investigate the systems implications of diversity embedded codes by examining value to network utility maximization, unequal error protection for wireless transmission, rate opportunism and packet delay optimization. [J314]

"Digital Rights Management and Individualized Pricing"

Digital rights management makes it easier for vendors to practice price discrimination online. Public resistance is perhaps the main reason it is not prevalent in online information sales. [J315]

"Searching for the Right Fit: Balancing IT Security Management Model Trade-Offs"

IT security professionals' effectiveness in an organization is influenced not only by how usable their security management tools are but also by how well the organization's security management model (SMM) fits. Finding the right SMM is critical but can be challenging-trade-offs are inherent to each approach, but their implications aren't always clear. The authors present a case study of one academic institution that created a centralized security team but disbanded it in favor of a more distributed approach three years later. They contrast these experiences with expectations from industry standards. [J316]

"Useful Computer Security"

Usability is a growing concern in designing systems and applications that operate securely. Most usability work has focused on improving user interfaces, but security is systemic, and negotiating, instituting, and maintaining real-world security procedures and practices is an organizational and social activity. [J317]

"Wind Power [Ja review of Grid Integration of Wind Energy Conversion Systems (S. Heier; 2006); book review]"

This book contains engineering information about the operating principles, design, and application of wind turbines. Grid integration is covered in much less depth and is largely focused upon issues within the medium-voltage collector systems of multi-unit wind farms. Topics covered include power-electronic converter systems, harmonics, filter design, and protection. The book is well suited as a text or reference book for engineering students or researchers. It would also be very useful to wind turbine designers, who need detailed equations and graphs to understand the intricate technical issues related to energy conversion or turbine components. [J318]

"Challenges in Certification and Accreditation"

As the threat of malicious activity through the Internet increased, the US government began reviewing protection requirements for national and international security systems. Legislation resulting from this review included the Federal Information Security Management Act (FISMA), the Paperwork Reduction Act of 1995, and the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act). This legislation sought to foster trust between the government and the public through significant security improvements in these systems. To this end, it the government established a peer-review process we've come to know as certification and accreditation, or C&A. [J319]

"Information and Quality Assurance: An Unsolved, Perpetual Problem for Past and Future Generations"

Quality assurance is well understood in the hardware/manufacturing community but not necessarily within the software community. The meaning of Information assurance depends on who you ask; those in the computer security field interpret information assurance as the need to protect the information, those in quality assurance relate information assurance to the quality of the information. Software assurance ranks even poorer in understanding; although most would agree that it relates to quality, they would be unsure what that means. System assurance is well understood due to its basis on known systems-engineering principles, tending to emphasize the dichotomy of hardware and software concept understanding. In this issue, three articles address parts of the assurance puzzle, which includes: quality assurance, information assurance, software assurance, and system assurance. The combination of these four builds the argument for trust, which is the sole reason for building assurances. To help avoid costly mismatches, consider looking at which part of the assurance puzzle you need solved first before looking at supposed assurance solutions. [J320]

"A New Shared Segment Protection Method for Survivable Networks with Guaranteed Recovery Time"

Shared segment protection (SSP), compared with shared path protection (SPP), and shared link protection (SLP), provides an optimal protection configuration due to the ability of maximizing spare capacity sharing, and reducing the restoration time in cases of a single link failure. This paper provides a thorough study on SSP under the GMPLS-based recovery framework, where an effective survivable routing algorithm for SSP is proposed. The tradeoff between the price (i.e., cost representing the amount of resources, and the blocking probability), and the restoration time is extensively studied by simulations on three networks with highly dynamic traffic. We demonstrate that the proposed survivable routing algorithm can be a powerful solution for meeting stringent delay upper bounds for achieving high restorability of transport services. This can significantly improve the network reliability, and enable more advanced, mission critical services in the networks. The comparison among the three protection types further verifies that the proposed scheme can yield significant advantages over shared path protection, and shared link protection. [J321]

"Recent progress in dynamic routing for shared protection in multidomain networks"

A large number of studies on routing for shared protection focus on minimizing the network transport capacity in a static routing framework. A smaller number of studies have been conducted on dynamic routing. Most of them do not meet the scalability requirements of multidomain networks. This article reviews the recent works in dynamic routing for shared protection in multidomain networks, and proposes a quantitative comparison among the most efficient approaches. Some of the remaining challenges are discussed at the end of the article. [J322]

"IEEE-USA-Supported Genetic-information Nondiscrimination Act Signed into Law [JIEEE-USA]"

{no data available} [J323]

"Home gateway operating model using reference monitor for enhanced user comfort and privacy"

In home network environments, user comfort and privacy are key prerequisites for customer satisfaction and data security. Although methods such as ACLs and others control the user-access for home network devices, most existing methods have yet to satisfactorily address the issues related to a user's comfort level and his or her protection of privacy. Therefore, this paper outlines the proposal for home gateway operating model using reference monitor in an OSGi service platform, whose goal is to enhance the operation required to efficiently meet a user's access, convenience, and privacy concerns. The reference monitor is a collection of access controls for objects, and is also capable of providing the facilities for access control. Furthermore, it adds the element of comfort to user access control, because it is intended as a core part of how subjects interact with objects. The proposed model is based on an RBAC model to effectively manage access control. Its policy is classified into two types (e.g., user-role assignment policy and permission-role assignment policy) in an attempt to not only better protect user privacy, but also to improve the performance of the policy operation. It is argued that the new home gateway model provides sufficient and effective guidelines to suggest future access control policies. [J324]

"A Security Mechanism of Web Services-Based Communication for Wind Power Plants"

The IEC 61400-25 standard has defined the mapping of wind power-plant information model to Web services (WS). Ensuring the security of WS-based communication for wind power plants is an unsolved problem. WS-security is a standard used to deal with the security requirements in applications of Web services, while the username/password and X.509 certificates are security tokens most commonly used in electric power utilities. We propose a security mechanism that deals with the requirements of authentication, integrity, nonreputation, and confidentiality across the communication process based on WS-Security and the two security tokens. The

security mechanism is implemented by an extension of simple object-access protocol message, design of the security agent, and the related security message-processing algorithm. An instance is modeling based on IEC 61400-25 to demonstrate the security-enhanced remote control of wind power plants. The result supports the usefulness of the security mechanism for WS-based wind power plants communication. [J325]

"Differential diversity-embedding space-time block coding for 2 and 4 transmit antennas"

Diversity-embedding space-time block coding (DE-STBC), introduced in the work of Diggavi et al. (2003), enables unequal error protection (UEP) using multiple transmit antennas. Even though these codes do not require channel state information (CSI) at the transmitter, they do need it at the receiver for decoding. A novel differential DE-STBC scheme is proposed in this paper to eliminate the need for channel estimation at the receiver which is especially costly with multiple transmit and receive antennas. Most previously proposed differential schemes in the literature are based on orthogonal STBC and hence are not applicable to the non-orthogonal family of DE-STBC considered in this paper. [J326]

"Analysis of the Hash Function Design Strategy Called SMASH"

The hash function design strategy SMASH was recently proposed as an alternative to the MD4 family of hash functions. It can be shown that the strategy leads to designs that are vulnerable to efficient collision and (second) preimage attacks. The mathematical structure of the SMASH description facilitates the description of the weakness and the resulting attacks, but also functions with less mathematical elegance may show similar weaknesses. [J327]

"SIISAM: A Model for Secure Inhomogeneous Information Systems"

SIISAM is a multilayered, Web-service-based architecture model designed to guide construction of a secure, interoperable, and extensible information system that allows smooth interoperation of legacy applications. A pilot e-government system in China built using the model has achieved its targets in both functionality and performance. [J328]

"Open DRM and the Future of Media"

Consumers want to use their digital content in the same way they have always used analog content. Consumer associations and governments are starting to request and even impose interoperability between DRM vendors' products. Therefore, interoperability has become a hot topic among content creators and distributors. Digital music providers and even authors are starting to refute the idea thatDRM is an ideal solution for protecting their rights. This is partly due to Apple and Microsoft not making their solutions interoperate. [J329]

"Error Exponent Regions for Gaussian Broadcast and Multiple-Access Channels"

In modern communication systems, different users have different requirements for quality of service (QoS). In this work, QoS refers to the average codeword error probability experienced by the users in the network. Although several practical schemes (collectively referred to as unequal error protection schemes) have been studied in the literature and are implemented in existing systems, the corresponding performance limits have not been studied in an information-theoretic framework. In this paper, an information-theoretic framework is considered to study communication systems which provide heterogeneous reliabilities for the users. This is done by defining individual probabilities of error for the users in the network and obtaining the fundamental tradeoffs of the corresponding error exponents. In particular, we quantify the reliability tradeoff by introducing the notion of error exponent region (EER), which specifies the set of error exponent vectors that are simultaneously achievable by the users for a fixed vector of users' rates. We show the existence of a tradeoff among the users' error exponents by deriving inner and outer bounds for the EER. Using this framework, a system can be realized, which can provide a tradeoff of reliabilities among the users for a fixed vector of users' rates. This adds a completely new dimension to the performance tradeoff in such networks, which is unique to multiterminal communication systems, and is beyond what is given by the conventional performance-versus-rate tradeoff in single-user systems. Although this is a very general concept and can be applied to any multiterminal communication system, in this paper we consider Gaussian broadcast and multiple-access channels (MACs). [J330]

"NTRUSign With a New Perturbation"

NTRUSign, a digital signature scheme, is suffering an effective attack. In this correspondence, we insert a new perturbation into NTRUSign primitive. With the new perturbation, each signature value is a linear combination of the private keys, and the combination coefficients have a hidden distribution. By a large number of signatures,

the attacker obtains the value of some complicated function of the private keys. It appears as hard problem computing the private keys from this value. Our scheme is smaller in size, presents a higher efficiency, and provides a clearer security proof than NTRUSign with the old perturbation. [J331]

"Security threats in wireless sensor networks"

First Page of the Article [J332]

"Guest Editors' Introduction: Special Section on Intelligence and Security Informatics"

The 12 papers in this special section focus on intelligence and security informatics. They are summarized here. [J333]

"Silver Bullet Security Podcast Series"

{no data available} [J334]

"Public health information infrastructure"

The public health infrastructure is a set of agencies and organizations whose mission is to create the environment in which we can be healthy. This broadest of definitions includes state and local health departments, selected federal agencies, and a wide range of other governmental, nonprofit, and for-profit agencies and organizations. This report will limit itself to state and local health departments and the federal Centers for Disease Control and Prevention (CDC), the nation's foremost public health agency. With numerous exceptions, this public health infrastructure is in a state of crisis, incapable of meeting our collective needs for public health protections and services, and likely to get worse in the near-term future. [J335]

"Privacy: A non-existent entity"

The development and implementation of new technologies has led to a significant erosion of privacy. In this circumstance, it is an arduous struggle to control one's personal information. Now we need to determine the best ways to protect individuals from abuse when their personal information is collected and distributed. [J336]

"News Briefs"

This paper deals with an algorithm that generates useful blacklists for networks by taking information from victims of past network attacks and predicting which hacker sites are likely to target specific networks in the future. Blacklists, which contain IP addresses previously involved in malicious activity, are an increasingly popular security technique. However, there are problems with the two main blacklisting approaches. HPB uses two analysis engines to create a blacklist for each network it protects. One engine ranks attack sources based on their relevance to the network for which it is developing a blacklist. The other determines the severity of potential attacks. The highly predictive blacklist approach works with information about harmful online activity that the SANS Institute collects via its DShield system. After filtering out unnecessary information, HPB runs the data through one system that ranks attack sources based on their relevance to a network being protected and one that determines potential attack severity. [J337]

"Vector Watermarking Robust to Both Global and Local Geometrical Distortions"

A blind watermarking algorithm for vector graphic images is presented. The algorithm is resilient to both global and local geometrical distortions. The polygonal line is represented by the wavelet descriptor. An additive watermarking scheme is used to embed the watermark by slightly modifying the wavelet descriptor, and that causes invisible distortions to the coordinates of the vertices. The invariant properties of the wavelet descriptor ensure that the presented algorithm is resilient against both global and local geometrical distortions. Using vector graphic images from contour maps, we demonstrate that the presented algorithm outperforms the algorithm based on the Fourier descriptor. [J338]

"The Gaussian Multiple Access Wire-Tap Channel"

We consider the Gaussian multiple access wire-tap channel (GMAC-WT). In this scenario, multiple users communicate with an intended receiver in the presence of an intelligent and informed wire-tapper who receives a degraded version of the signal at the receiver. We define suitable security measures for this multiaccess environment. Using codebooks generated randomly according to a Gaussian distribution, achievable secrecy rate regions are identified using superposition coding and time-division multiple access (TDMA) coding schemes. An

upper bound for the secrecy sum-rate is derived, and our coding schemes are shown to achieve the sum capacity. Numerical results are presented showing the new rate region and comparing it with the capacity region of the Gaussian multiple-access channel (GMAC) with no secrecy constraints, which quantifies the price paid for secrecy. [J339]

"Improving Behavioral IO Buffer Modeling Based on IBIS"

High level behavioral modeling is widely used in lieu of low level transistor models to ascertain the behavior of input/output (IO) drivers and receivers. The input output buffer information specification (IBIS) is one of the most widely used methodologies to model IO drivers as it satisfies the basic requirements of a behavioral model such as IP protection, simple structure, fast simulation time, and reasonable accuracy. As driver technology gets increasingly complicated and rise time of input signal gets increasingly smaller, important considerations such as simultaneous switching noise (SSN) becomes a major consideration when simulating multiple IO drivers in the integrated circuit. Unfortunately, IBIS falls short of becoming a complete IO behavioral model when simulating for SSN. This paper addresses the problem by assessing what is missing in IBIS. A method is presented for compensating for the missing information by complimenting the IBIS model with a black box that is simulator independent, without compromising with the speed that IBIS enjoys over the transistor models. [J340]

"Multipurpose Watermarking Based on Multiscale Curvelet Transform"

Multipurpose watermarking for content authentication and copyright verification are accomplished by using the multiscale curvelet transform. A curvelet transform gains better and sparser representation than most traditional multiscale transforms. In this paper, an image is decomposed into multiscale coefficients with a dyadic number of wedges constructed from a variety of neighboring scales. Image hash is designed to extract image features from an approximate scale. The image features represented in the form of bit sequences are then embedded onto the wedges by a quantization based on human visual system behavior. The implementation strategy achieves content authentications for fatigue watermarking and copyright verifications for robust watermarking. The experiments demonstrate good results to support the feasibility of using this method in multipurpose applications. [J341]

"Bridging Security and Fault Management within Distributed Workflow Management Systems"

As opposed to centralized workflow management systems, the distributed execution of workflows can not rely on a trusted centralized point of coordination. As a result, basic security features including compliance of the overall sequence of workflow operations with the pre-defined workflow execution plan or traceability become critical issues that are yet to be addressed. Besides, the detection of security inconsistencies during the execution of a workflow usually implies the complete failure of the workflow although it may be possible in some situations to recover from the latter. In this paper, we present security solutions supporting the secure execution of distributed workflows. These mechanisms capitalize on onion encryption techniques and security policy models to assure the integrity of the distributed execution of workflows, to prevent business partners from being involved in a workflow instance forged by a malicious peer and to provide business partners identity traceability for sensitive workflow instances. Moreover, we specify how these security mechanisms can be combined with a transactional coordination framework to recover from faults that may be caught during their execution. The defined solutions can easily be integrated into distributed workflow management systems as our design is strongly coupled with the runtime specification of decentralized workflows. [J342]

"A novel scheme for protecting receiver's location privacy in wireless sensor networks"

Due to the open nature of a sensor network, it is relatively easy for an adversary to eavesdrop and trace packet movement in the network in order to capture the receiver physically. After studying the adversary's behavior patterns, we present countermeasures to this problem. We propose a locationprivacy routing protocol (LPR) that is easy to implement and provides path diversity. Combining with fake packet injection, LPR is able to minimize the traffic direction information that an adversary can retrieve from eavesdropping. By making the directions of both incoming and outgoing traffic at a sensor node uniformly distributed, the new defense system makes it very hard for an adversary to perform analysis on locally gathered information and infer the direction to which the receiver locates. We evaluate our defense system based on three criteria: delivery time, privacy protection strength, and energy cost. The simulation results show that LPR with fake packet injection is capable of providing strong protection for the receiveriquests location privacy. Under similar energy cost, the safe time of the receiver provided by LPR is much longer than other methods, including Phantom routing [1] and DEFP [2]. The performance of our system can be tuned through a few system parameters that determine the tradeoff between energy cost and the strength of location-privacy protection. [J343]

"Evaluation of breakdown characteristics of gas insulated switchgears for non-standard lightning impulse waveforms under diverse conditions"

To lower the lightning impulse withstand voltage of gas insulated switchgear (GIS) while maintaining the high reliability of its insulation performance, it is important to define in an organized way the insulation characteristics for non-standard lightning impulse voltage waveforms that represent actual surge waveforms in the field and compare them with the characteristics for the standard lightning impulse waveform quantitatively. In the preceding researches, the dielectric breakdown voltage-time characteristics were measured under several different conditions on the quasi-uniform SF6gas gap and partly the cone-shaped insulating spacers that represent an insulation element of GIS for six kinds of non-standard lightning impulse waveforms associated with lightning surges and disconnector switching surges. As a result, in the tested range, the dielectric breakdown values for non-standard lightning impulse waveforms were higher than those for the standard lightning impulse waveform by 3% to 36%. In these experiments, parameters other than waveforms were fixed to standard conditions. In this paper insulation characteristics on quasi-uniform SF6gas gaps were examined while changing conditions on gas pressures, gap lengths, electrode surface roughness, voltage polarities, and bias voltages. As a result, it was confirmed that the results under standard experimental conditions in the preceding experiments can be applied widely to the GIS actual equipment conditions. [J344]

"A Buyer-Seller Watermarking Protocol Based on Secure Embedding"

In a forensic watermarking architecture, a buyer-seller protocol protects the watermark secrets from the buyer and prevents false infringement accusations by the seller. Existing protocols encrypt the watermark and the content with a homomorphic public-key cipher and perform embedding under encryption. When used for multimedia data, these protocols create a large computation and bandwidth overhead. In this correspondence, we show that the same functionality can be achieved efficiently using recently proposed secure watermark embedding algorithms. [J345]

"Hierarchical Watermarking of Semiregular Meshes Based on Wavelet Transform"

This paper presents a hierarchical watermarking framework for semiregular meshes. Three blind watermarks are inserted in a semiregular mesh with different purposes: a geometrically robust watermark for copyright protection, a high-capacity watermark for carrying a large amount of auxiliary information, and a fragile watermark for content authentication. The proposed framework is based on wavelet transform of the semiregular mesh. More precisely, the three watermarks are inserted in different appropriate resolution levels obtained by wavelet decomposition of the mesh: the robust watermark is inserted by modifying the norms of the wavelet coefficient vectors associated with the lowest resolution level; the fragile watermark is embedded in the high resolution level obtained just after one wavelet decomposition by modifying the orientations and norms of the wavelet coefficient vectors; the high-capacity watermark is inserted in one or several intermediate levels by considering groups of wavelet coefficient vector norms as watermarking primitives. Experimental results demonstrate the effectiveness of the proposed framework: the robust watermark is able to resist all common geometric attacks even with a relatively strong amplitude; the fragile watermark is robust to content-preserving operations, while being sensitive to other attacks of which it can also provide the precise location; the payload of the high-capacity watermark increases rapidly along with the number of watermarking primitives. [J346]

"Identity management systems"

Most organizations have difficulty keeping track of and controlling all the user identifiers and passwords across their systems. Identity management (IdM) systems are designed to help manage user identifiers across multiple systems as well as providing a way to manage user access over their lifecycle of roles in the organization. They are tightly integrated with other systems such as those that provide a single sign-on mechanism and the checking of their credentials. As such, these IdM systems have become extremely common in information technology infrastructure. [J347]

"Information Integrity and IT Professionals' Integrity, Intertwined"

When a consumer accesses information, the consumer wants to trust that information. As computer professionals, our reputation with the public depends in large part on how the public perceives the information we deliver-if the public trusts the information, the public trusts us. This article focus on three threats to information integrity that map directly to three characteristics of information-processing professionals: incompetence, conflicts of interest, and a lack of transparency. In each case, characteristics of both individuals and the profession as a whole interact to undermine information integrity. The article concludes with strategies for improving information integrity by focusing on these three problems. [J348]

"IT as a Profession: Is Competent Creation the Primary Goal?"

This article introduces four articles on the general theme of IT professionalism that make up this special issue. The authors also critique the assertion by J. Steib that "the primary goal of professionalism is competent creation." The authors conclude that although competent creation is an important part of IT professionalism, it isn't primary. Instead, the public good is to be primary for IT professionals. [J349]

"A Privacy Preserving Repository for Data Integration across Data Sharing Services"

Current data sharing and integration among various organizations require a central and trusted authority to first collect data from all data sources and then integrate the collected data. This process tends to complicate the update of data and to compromise data sources' privacy. In this paper, a repository for integrating data from various data sharing services without central authorities is presented. The major differences between our repository and existing central authorities are: 1) Our repository collects data from data sharing services based on users' integration requirements rather than all the data from the data sharing services as existing central authorities. 2) While existing central authorities have full control of the collected data, the capability of our repository is restricted to computing the integration results required by users and cannot get other information about the data or use it for other purposes. 3) The data collected by our repository cannot be used to generate other results except that of the specified data integration request, and hence the compromise of our repository can only reveal the results of the specified data integration request, while the compromise of central authorities will reveal all data. [J350]

"The Crutial Way of Critical Infrastructure Protection"

Critical infrastructures such as the power grid are essentially physical processes controlled by computers connected by networks. They're usually as vulnerable as any other interconnected computer system, but their failure has a high socioeconomic impact. The Critical Utility Infrastructural Resilience (Crutial) project designed an information switch (CIS) to protect these infrastructures. These devices help ensure that incoming and outgoing traffic satisfies the security policy of an infrastructure in face of cyberattacks. A CIS isn't a firewall, but a distributed protection device based on a sophisticated access control model. Furthermore, a CIS is intrusion-tolerant and self-healing, seeking perpetual unattended correct operation. [J351]

"Vulnerability Assessment for Critical Infrastructure Control Systems"

Assessing security in critical control systems is a particular task that can have dangerous real-world consequences if done poorly or according to more traditional security assessments. In 2006, the North American Electric Reliability Corporation adopted the Critical Infrastructure Protection standards for cyber vulnerability assessment of critical infrastructure control systems. Such CIP assessments entail challenges at each stage, from planning and assessing to reporting results and recommending vulnerability mitigation approaches. [J352]

"Process Control System Security: Bootstrapping a Legacy"

Internet connectivity is just one of the concerns that has led to an increased focus on improving cyber security protection in process or industrial control systems. In this special issue, a vendor reviews the concerns and researchers provide recommendations that can lead to improved security. [J353]

"Secure user identification for consumer electronics devices"

With the evolution of consumer electronics technologies, personal information in consumer devices is becoming increasingly valuable. To protect private information from misuses due to loss or theft, secure user identification mechanisms should be equipped into the consumer devices. This paper develops a secure user identification system for consumer electronics devices based on fingerprint identification. The fingerprint identification system is one of the biometric sensor technologies, which provides high accuracy and convenience than other identification techniques. Specifically, the proposed system uses the orientation map and the edit-distance for immediate and accurate identification of users. Experimental results show that the proposed system achieves good performance in terms of the false rejection rate and the false acceptance rate. [J354]

"Secure vehicular communication systems: design and architecture"

Significant developments have taken place over the past few years in the area of vehicular communication systems. Now, it is well understood in the community that security and protection of private user information are a prerequisite for the deployment of the technology. This is so precisely because the benefits of VC systems, with the mission to enhance transportation safety and efficiency, are at stake. Without the integration of strong

and practical security and privacy enhancing mechanisms, VC systems can be disrupted or disabled, even by relatively unsophisticated attackers. We address this problem within the SeVeCom project, having developed a security architecture that provides a comprehensive and practical solution. We present our results in a set of two articles in this issue. In this first one, we analyze threats and types of adversaries, identify security and privacy requirements, and present a spectrum of mechanisms to secure VC systems. We provide a solution that can be quickly adopted and deployed. In the second article we present our progress toward the implementation of our architecture and results on the performance of the secure VC system, along with a discussion of upcoming research challenges and our related current results. [J355]

"Protected core networking: an architectural approach to secure and flexible communications"

Protected core networking (PCN) is a concept intended to be used to implement a flexible transport infrastructure that supports future military operations based on network enabled capability (NEC). PCN is based on creating a loose coupling between information domains and the transport infrastructure, and focusing on the provision of high service availability, also in high-threat environments. This architectural approach highlights a number of emerging and novel concepts where research and development is needed to properly support NEC. [J356]

"A novel selected mapping technique for PAPR reduction in OFDM systems"

Selected mapping (SLM) is a well-known method for reducing the peak-to-average power ratio (PAPR) in orthogonal frequency-division multiplexing (OFDM) systems. The main drawback of this technique is that, for each data block, it requires the transmission of several side information bits, which results in some data rate loss. These redundant bits are so critical to the error performance of the system that they need in practice to be protected by a powerful channel code. This increases the system complexity and transmission delay, and decreases the data rate even further. In this paper, we propose a novel SLM method for which no side information needs to be sent. By considering the example of an OFDM system using 16-QAM modulation, it is shown that the proposed method performs very well both in terms of PAPR reduction and bit error rate at the receiver output. [J357]

"Multimodal biometric authentication using teeth image and voice in mobile environment"

Mobile devices such as smart-phone, PDA and mobile-phone are vulnerable to theft and loss due to their small size and the characteristics of the environments in which they are used. A simple and convenient authentication system is required to protect private information stored in the mobile device. Therefore, we propose a new multimodal biometric authentication approach using teeth image and voice as biometric traits in this paper. The individual matching scores obtained from the teeth image and voice are combined using a weighted-summation operation, and the fused-score is utilized to classify an unknown user into the acceptance or rejection. The proposed method is evaluated using 1000 teeth images and voices, in which these are collected by smart-phone, i.e., one mobile device for 50 subjects. In the experiment results, the proposed method has an EER of 2.13%, and we demonstrate the effectiveness of the proposed method. [J358]

"A Secure Information Flow Architecture for Web Service Platforms"

Current Web service platforms (WSPs) often perform all Web services-related processing, including security-sensitive information handling, in the same protection domain. Consequently, the entire WSP may have access to security-sensitive information, forcing us to trust a large and complex piece of software. To address this problem, we propose ISO-WSP, a new information flow architecture that decomposes current WSPs into a small trusted T-WSP to handle security-sensitive data and a large, legacy untrusted U-WSP that provides the normal WSP functionality. To achieve end-to-end security, the application code is also decomposed into a small trusted part and the remaining untrusted code. The trusted part encapsulates all accesses to security-sensitive data through a secure functional interface (SFI). To ease the migration of legacy applications to ISO-WSP, we developed tools to translate direct manipulations of security-sensitive data by the untrusted part into SFI invocations. Using a prototype implementation based on the Apache Axis2 WSP, we show that ISO-WSP reduces software complexity of trusted components by a factor of five, while incurring a modest performance overhead of few milliseconds per request. We also show that existing applications can be migrated to run on ISO-WSP with a few tens of lines of new and modified code. [J359]

"Secure vehicular communication systems: implementation, performance, and research challenges"

Vehicular communication systems are on the verge of practical deployment. Nonetheless, their security and privacy protection is one of the problems that have been addressed only recently. In order to show the feasibility of secure VC, certain implementations are required. we discuss the design of a VC security system that has

emerged as a result of the European SeVe-Com project. In this second article we discuss various issues related to the implementation and deployment aspects of secure VC systems. Moreover, we provide an outlook on open security research issues that will arise as VC systems develop from today's simple prototypes to full-fledged systems. [J360]

"Systematic Study of the Urban Postconflict Change Classification Performance Using Spectral and Structural Features in a Support Vector Machine"

The state of built-up features after their destruction, as well as the process of their rehabilitation, are assessed through the analysis of conflict and postconflict very high spatial resolution Ikonos images using a pixel-level support vector machine (SVM) learning classification approach. Different input vectors of the supervised SVM classifier are tested in order to assess the discrimination power of structural and spectral image descriptors: the use of spectral information only with (a) the panchromatic images at time t0and t1, (b) the pan-sharpened images with the multispectral bands at time t0and t1, (c) the iteratively re-weighted multivariate alteration detection (IR-MAD) variates derived from dataset (b); the use of structural information only with image series resulting from the decomposition by the derivative of the morphological profile (DMP) of the panchromatic (d) and pan-sharpened (e) data; finally, the use of spectral and structural information simultaneously (f) and (g) by stacking up (a) and (d), and (b) and (e), respectively. The results show that the SVM performs better with feature vectors based on the simultaneous use of spectral and structural information rather than with those formed by the grey-level information or the DMPs only. Moreover, approach (f) requiring only two panchromatic data as input compete well with approaches (b), (e), and (g), which instead necessitate ten spectral channels as input. [J361]

"Combined puncturing and path pruning for convolutional codes and the application to unequal error protection"

In this paper, puncturing and path pruning are combined for convolutional codes to construct a new coding scheme for unequal error protection (UEP), called the hybrid punctured and path-pruned convolutional codes. From an algebraic viewpoint, we show that the hybrid codes not only inherit all the advantages of the conventional rate-compatible punctured convolutional codes and path-compatible pruned convolutional codes but also can provide more flexible choices of protection capability for UEP. In addition, a data-multiplexing scheme originally proposed for path-pruned codes which can guarantee smooth transition between rates without additional zero-padding for frame termination is proven applicable to the hybrid codes to improve the system throughput. [J362]

"New Technology Prevents Data Leakage"

Security experts are working on data-leak-prevention technology to combat threats emanating from employees and others deliberately or inadvertently sending out sensitive material without authorization. [J363]

"Choosing a Security Option: The InfoSecure Methodology"

A four-step process can help organizations evaluate assets to be protected, potential assailants, and likely methods and tactics. It then pulls the results together as a plan of action for investing in cybersecurity in ways that protect the most critical organizational information and processes. [J364]

"Silver Bullet Security Podcast series"

{no data available} [J365]

"A New Strategy for Determining Fault Zones in Distance Relays"

A new strategy (denoted P-SS) for estimating the correct fault zone in distance relays is introduced. The main difference between the P-SS and conventional setting strategies is that the P-SS does not depend on fixed boundaries for backup zones. It depends on exchanging information between local relays in the same station in addition to a command from the remote end relay. With the proposed strategy, zone-1 covers the entire length of the protected line, zone-2 covers the entire length of any next line irrespective of its length, and zone-3 covers the entire length of any line next to zone-2. The governing rules for the proposed strategy are presented. The strategy is examined against a wide range of setting problems of a real part of a high-voltage network with real relay settings. The results confirm that the P-SS achieves the required accurate, sensitive, and selective relay operation. [J366]

"Gaining a Wider Perspective"

The recent world-wide rash of power systems blackouts has provided an added impetus to wide-scale deployment of phasor measurement units (PMUs). Initial applications of PMUs in the late 1980s and 1990s were isolated due to the limited infrastructure availability and lack of computational support for extensive processing of the networked information. Today, networks of hundreds of PMUs are in place and more are planned.The recognition that networks of PMUs can provide greater power system reliability is based on their ability to give direct access to the state of the power system at any given instant. [J367]

"Silver Bullet Security Podcast series"

{no data available} [J368]

"Index Assignment for Quantized Beamforming MIMO Systems"

Index assignment (IA) technique is introduced to quantized beamforming systems. The feedback channel in these systems is modeled as a discrete memoryless channel (DMC), and the diversity and array gains with feedback errors are derived. Based on the analytical results, IA scheme is designed to provide a redundancy-free protection against feedback errors. Simulation results show that good IA scheme improves the array gain and symbol error rate (SER). [J369]

"Systematic Lossy Error Protection of Video Signals"

This paper proposes a scheme called systematic lossy error protection (SLEP) for robust transmission of video signals over packet erasure channels. The systematic portion of the transmission consists of a conventionally encoded video bit stream which is transmitted without channel coding. An additional bit stream generated by Wyner-Ziv encoding of the video signal is transmitted for error resilience. In the event of packet loss, this supplementary bit stream is decoded and allows the recovery of a coarsely quantized video signal, which is displayed in lieu of the lost portions of the primary video signal. The quantization mismatch results in a small, controlled loss in picture quality, but a drastic reduction in picture quality is avoided. An implementation of the SLEP system using the state-of-the-art H.264/AVC standard codec is described. Specifically, H.264/AVC redundant slices are used in conjunction with Reed-Solomon coding to generate the Wyner-Ziv bit stream. The received video quality is modeled as a function of the bit rates of the primary and redundant descriptions and the error resilience bit rate. The model is used to optimize the video quality delivered by SLEP. Via theoretical analysis and experimental simulation, it is shown that SLEP provides a flexible tradeoff between error resilience and decoded picture quality. By allowing the quality to degrade gracefully over a wider range of packet loss rates, SLEP mitigates the precipitous drop in picture quality suffered by traditional FEC-based systems. [J370]

"Silver Bullet Security Podcasts"

{no data available} [J371]

"Design and simulation of a grounding grid for GIS substation"

A grounding grid is designed with the capacity to minimize the very fast transient overvoltage generated during switching operations in a Gas Insulated Substation (GIS). The methodology takes the reference from the IEEE Std. 80-2000 and contains detailed models of GIS and grounding grid. By means an iterative process, new elements are added to the grounding grid for reducing magnitude of a very fast transient overvoltage in different points of a substation. This permits to improve the levels of personal security and the protection of apparatus in the substation. [J372]

"Nice Error Bases and Sylow Subgroups"

Nice error bases have various applications in quantum computing such as in the teleportation of quantum states and in the theory of noiseless systems. Associated in a natural way to any nice error basis there is a so-called index group and also a group of central type. In this paper, we will extend the number of known index groups for nice error bases by exploiting the connections between groups of central type and their Sylow subgroups. Our methods will allow us find all index groups of degree up to 44 with two exceptions. [J373]

"Vulnerability Assessment of Cybersecurity for SCADA Systems"

Vulnerability assessment is a requirement of NERC's cybersecurity standards for electric power systems. The purpose is to study the impact of a cyber attack on supervisory control and data acquisition (SCADA) systems. Compliance of the requirement to meet the standard has become increasingly challenging as the system

becomes more dispersed in wide areas. Interdependencies between computer communication system and the physical infrastructure also become more complex as information technologies are further integrated into devices and networks. This paper proposes a vulnerability assessment framework to systematically evaluate the vulnerabilities of SCADA systems at three levels: system, scenarios, and accesspoints. The proposed method is based on cyber systems embedded with the firewall and password models, the primary mode of protection in the power industry today. The impact of a potential electronic intrusion is evaluated by its potential loss of load in the power system. This capability is enabled by integration of a logic-based simulation method and a module for the power flow computation. The IEEE 30-bus system is used to evaluate the impact of attacks launched from outside or from within the substation networks. Countermeasures are identified for improvement of the cybersecurity. [J374]

"A Secure Authentication Scheme with Anonymity for Wireless Communications"

Recently, a new authentication scheme with anonymity for wireless communications has been proposed, and then some security problems have been demonstrated. In this paper, we will discuss a few problems found in the enhanced scheme and then propose how to overcome them, regarding the properties of anonymity and backward secrecy. [J375]

"Hardening the Target"

As enterprises increasingly depend on digitized data and seek commercial opportunities from accelerated digital access and transmission, senior management and boards of directors haven't sufficiently updated their enterprises' security protections on digitally stored information. Consequently, new and increasingly frequent attacks have occurred against their digital information assets. Enterprises must "harden the target" to protect against attacks against these assets. [J376]

"Embedded Rank Distance Codes for ISI Channels"

Designs for transmit alphabet constrained space-time codes naturally lead to questions about the design of rank distance codes. Recently, diversity embedded multilevel space-time codes for flat-fading channels have been designed from sets of binary matrices with rank distance guarantees over the binary field by mapping them onto quadrature amplitude modulation (QAM) and phase-shift keying (PSK) constellations. In this paper, we demonstrate that diversity embedded space-time codes for fading intersymbol interference (ISI) channels can be designed with provable rank distance guarantees. As a corollary, we obtain an asymptotic characterization of the fixed transmit alphabet rate-diversity tradeoff for multiple antenna fading ISI channels. The key idea is to construct and analyze properties of binary matrices with a particular structure (Toeplitz structure) induced by ISI channels. [J377]

"Security and Privacy in Distributed Smart Cameras"

Distributed smart camera systems are becoming increasingly important in a wide range of applications. As they are often deployed in public space and/or our personal environment, they increasingly access and manipulate sensitive or private information. Their architectures need to address security and privacy issues appropriately, considering them from the inception of the overall system structure. In this paper, we present security and privacy issues of distributed smart camera systems. We describe security requirements, possible attacks, and common risks, analyzing issues at the node and at the network level and presenting available solutions. Although security issues of distributed smart cameras are analogous to networked embedded systems and sensor networks, emphasis is given to special requirements of smart camera networks, including privacy and continuous real-time operation. [J378]

"Smart Camera Based Monitoring System and Its Application to Assisted Living"

Western societies are aging rapidly. An automated 24/7 surveillance to ensure safety of the elderly while respecting privacy becomes a major challenge. At the same time this is representative of novel and emerging video surveillance applications discovered lately besides the classic surveillance protection applications in airports, government buildings, and industrial plants. Three problems of current surveillance systems are identified. A distributed and automated smart camera based approach is proposed that addresses these problems. The proposed system's goal set is to analyze the real world and reflect all relevant-and only relevant-information live in an integrated virtual counterpart for visualization. It covers georeferenced person tracking and activity recognition (falling person detection). A prototype system installed in a home for assisted living has been running 24/7 for several months now and shows quite promising performance. [J379]

"Cross-Border Data Flows and Increased Enforcement"

The term "privacy" is subject to many definitions and descriptions. Privacy is the subjective condition people experience when they have the power to control information about themselves and when they exercise that power consistent with their interests and values. The EU Data Protection Directive takes a somewhat different tack and defines personal data as data relating to an identified or identifiable individual, and then allocates a series of rights to the individual regarding the data, particularly regarding notice, consent, and other principles intended to grant an individual reasonable control over the data. [J380]

"Digital rights management for the home TV based on scalable video coding"

In this paper, the business model and digital rights management (DRM) solution are proposed for the home TV based on scalable video coding and convergent networks. In this environment, the TV program is broadcasted via digital video broadcasting for handheld terminals (DVB-H) to mobile phones, the access right is transmitted by Global System for Mobile communication (GSM/GPRS) channel, and the TV program can also be transmitted from mobile phones to home TV through WiFi. The typical application scenario is that the TV program with low quality (base layer) in the mobile phone can be enriched by enhancement information and shown on home TV. The business model is presented to pay for the enhancement information, and the DRM solution is proposed for solving the copyright issues in the convergence between the DVB-H broadcasting, GSM/GPRS and home network. Since few work has been done to solve this problem, the work proposed in this paper is expected to attract more researchers. [J381]

"Spatial Partitioning in Self-Organizing Smart Camera Systems"

We propose a decentralized, self-organizing system architecture for wireless networked smart cameras (SCs) with pan, tilt, and zoom abilities. Each SC communicates with its neighbors and independently calculates the optimal position for its field of view. Thereby, SCs autonomously organize themselves and spatially partition the area they observe. This is achieved by a decentralized algorithm that makes way for self-organization in SC systems. The system quickly adapts to new situations caused by joining and failing nodes. Simulations with hundreds of cameras show that scalability and reliability are achieved. We analyze the performance of different camera densities and show that optimal surveillance coverage is achieved in a short time (20 s) while maintaining low communication traffic using a simulated 350-node outdoor SC system. [J382]

"When Black Hats Are Really White"

Each August, more than 4,000 IT administrators, industry experts, government officials, and hackers gather at a convention in Las Vegas. The Black Hat Briefings (www.blackhat.com), as that conference is known, started out many years ago as a hacker's convention, but it has evolved into the premier venue for technical information on cybersecurity and the latest security research. [J383]

"Information Assurance Education: A Work In Progress"

The recognition that we need improved computer security education has increased over the past several years. Recent cyberattacks in Georgia and Estonia exemplify the new threats faced by economies that rely on the Internet. Thus, more people see the need to protect cyberspace-which translates into improving computer security in all aspects of computer use-as crucial for everyone, not merely for those who work with technology. In this column, we reflect on emerging opportunities and challenges in instruction as well as the need for increasing the partnerships among industry, government, and academia to foster mutual understanding of challenges and joint participation in solutions. [J384]

"Performance Metrics for Information Security Risk Management"

Qualitative methods are available for risk management, but better practice would use quantitative risk management based on expected losses and related metrics. Measuring the success of information security investments is best accomplished by measuring reductions in expected loss. [J385]

"Energy-Constrained Distortion Reduction Optimization for Wavelet-Based Coded Image Transmission in Wireless Sensor Networks"

Image transmissions in wireless multimedia sensor networks (WMSNs) are often energy constrained. They also have requirement on distortion minimization, which may be achieved through unequal error protection (UEP) based communication approaches. In related literature with regard to wireless multimedia transmissions, significantly different importance levels between image-pixel-position information and image-pixel-value

information have not been fully exploited by existing UEP schemes. In this paper, we propose an innovative image-pixel-position information based resource allocation scheme to optimize image transmission quality with strict energy budget constraint for image applications in WMSNs, and it works by exploring these uniquely different importance levels among image data streams. Network resources are optimally allocated cross PHY, MAC and APP layers regarding inter-segment dependency, and energy efficiency is assured while the image transmission quality is optimized. Simulation results have demonstrated the effectiveness of the proposed approach in achieving the optimal image quality and energy efficiency. The performance gain in terms of distortion reduction is especially prominent with strict energy budget constraints and lower image compression ratios. [J386]

"Entropy Analysis and New Constructions of Biometric Key Generation Systems"

In this paper, a new, soft two-level approach for the generation of multiple and revocable biometric keys, adapted to the analog nature of biometric signals, is proposed. It consists of a novel randomized soft code-offset construction for the Euclidean metric, at the first level, and a code-redundancy construction for the Hamming metric, possibly based on a Reed-Solomon code, at the second level. The Shannon entropy analysis shows that the new construction achieves optimal security with respect to biometric template protection, whereas the previously proposed constructions for the Euclidean metric are shown to be insecure in the multiple-key setting. In addition, a general code-offset construction for the Hamming metric is analyzed in terms of the Shannon entropy instead of the usual min entropy. This allows a nice characterization of the codes that provide biometric template protection in the multiple-key scenario as well as a further differentiation among these codes with respect to the achievable security level. [J387]

"Tolerance of intentional attacks in complex communication networks"

Motivated by recent developments in the theory of complex networks, we examine the tolerance of communication networks for intentional attacks that aim to crash the network by taking down network hubs. In addition to providing a brief survey of key existing results, we investigate two different effects that largely have been ignored in past studies. Many communication networks, such as the Internet, are too large for anyone to have global information of their topologies, which makes accurate, intentional attacks virtually impossible; most attacks in communication networks must propagate from nodes to adjacent nodes, utilizing local-network topology information only. We show that incomplete global information has a different impact on intentional attacks in different circumstances, and local information-based attacks can actually be highly efficient. Such insights will be helpful for the future development of efficient protection schemes against network attacks. [J388]

"Security Requirements for the Rest of Us: A Survey"

Most software developers aren't primarily interested in security. For decades, the focus has been on implementing as much functionality as possible before the deadline, and patching the inevitable bugs when it's time for the next release or hot fix. However, the software engineering community is slowly beginning to realize that information security is also important for software whose primary function isn't related to security. Security features or mechanisms typically aren't prominent in such software's user interface. [J389]

"Turbo Coded OFDM for Reducing PAPR and Error Rates"

A selective-mapping (SLM) scheme which does not require the transmission of side information and can reduce the peak to average power ratio (PAPR) in turbo coded orthogonal frequency-division multiplexing (OFDM) systems is proposed. The candidates of the proposed SLM are respectively generated by a turbo encoder using various interleavers. The waiver of side information can avoid the degradation of error rate performance which results from the incorrect recovery of side information at receiver in the conventional SLM OFDM system. [J390]

"Context-Aware Adaptation of Access-Control Policies"

Today, public-service delivery mechanisms such as hospitals, police, and fire departments rely on digital generation, storage, and analysis of vital information. To protect critical digital resources, these organizations employ access-control mechanisms, which define rules under which authorized users can access the resources they need to perform organizational tasks. Natural or man-made disasters pose a unique challenge, whereby previously defined constraints can potentially debilitate an organization's ability to act. Here, the authors propose employing contextual parameters-specifically, activity context in the form of emergency warnings-to adapt access-control policies according to a priori configuration. [J391]

"A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking"

Tracing IP packets to their origins is an important step in defending Internet against denial-of-service attacks. Two kinds of IP traceback techniques have been proposed as packet marking and packet logging. In packet marking, routers probabilistically write their identification information into forwarded packets. This approach incurs little overhead but requires large flow of packets to collect the complete path information. In packet logging, routers record digests of the forwarded packets. This approach makes it possible to trace a single packet and is considered more powerful. At routers forwarding large volume of traffic, the high storage overhead and access time requirement for recording packet digests introduce practicality problems. In this paper, we present a novel scheme to improve the practicality of log-based IP traceback by reducing its overhead on routers. Our approach makes an intelligent use of packet marking to improve scalability of log-based IP traceback. We use mathematical analysis and simulations to evaluate our approach. Our evaluation results show that, compared to the state-of-the-art log-based approach called hash-based IP traceback, our approach maintains the ability to trace single IP packet while reducing the storage overhead by half and the access time overhead by a factor of the number of neighboring routers. [J392]

"Paired Subimage Matching Watermarking Method on Ordered Dither Images and Its High-Quality Progressive Coding"

In this paper, we present two novel robust methods for embedding watermarks into dithered halftone images. The first method is named paired subimage matching ordered dithering (PSMOD), of which the decoder is provided with a priori information of the original watermark, and the corresponding application is copyright protection. The other method, blind paired subimage matching ordered dithering (BPSMOD), does not require the knowledge of the original watermark, and the main application is secret communication. Both methods utilize the bit and sub-subimage interleaving preprocesses. The experiments show that both techniques are sufficiently robust to guard against the cropping, tampering, and print-and-scan degradation processes, in either B/W or color dithered images. Both techniques are also sufficiently flexible for various levels of embedded capacities. Furthermore, a novel progressive coding scheme is also presented in this paper for the efficient display of dithered images. After the preprocessing of bit-interleaving, this algorithm utilizes the characteristic of reordered image to determine the transmitting order and then progressively reconstructs the dithered image. Moreover, the dithered images are further compressed by lossy and lossless procedures. The experimental results demonstrate high-quality reconstructions while maintaining low transmitted bit rates. [J393]

"Optimal Watermark Embedding and Detection Strategies Under Limited Detection Resources"

An information-theoretic approach is proposed to watermark embedding and detection under limited detector resources. First, the attack-free scenario is considered under which asymptotically optimal decision regions in the Neyman-Pearson sense are proposed, along with the optimal embedding rule. Later, the case of zero-mean independent and identically distributed (i.i.d.) Gaussian covertext distribution is explored with unknown variance under the attack-free scenario. For this case, a lower bound on the exponential decay rate of the false-negative probability is proposed. It is proven that the optimal embedding and detecting strategy is superior to the customary linear, additive embedding strategy in the exponential sense. Finally, these results are extended to the case of memoryless attacks and general worst case attacks. Optimal decision regions and embedding rules are offered, and the worst attack channel is identified. [J394]

"Diversity Embedded Space-Time Codes"

Rate and diversity impose a fundamental tradeoff in wireless communication. High-rate space-time codes come at a cost of lower reliability (diversity), and high reliability (diversity) implies a lower rate. However, wireless networks need to support applications with very different quality-of-service (QoS) requirements, and it is natural to ask what characteristics should be built into the physical layer link in order to accommodate them. In this paper, we design high-rate space-time codes that have a high-diversity code embedded within them. This allows a form of communication where the high-rate code opportunistically takes advantage of good channel realizations while the embedded high-diversity code provides guarantees that at least part of the information is received reliably. We provide constructions of linear and nonlinear codes for a fixed transmit alphabet constraint. The nonlinear constructions are a natural generalization to wireless channels of multilevel codes developed for the additive white Gaussian noise (AWGN) channel that are matched to binary partitions of quadrature amplitude modulation (QAM) and phase-shift keying (PSK) constellations. The importance of set-partitioning to code design for the wireless channel is that it provides a mechanism for translating constraints in the binary domain into lower bounds on diversity protection in the complex domain. We investigate the systems implications of embedded diversity codes by examining value to unequal error protection, rate opportunism, and packet delay optimization. These applications demonstrate that diversity-embedded codes have the potential to outperform traditional single-layer codes in moderate signal-to-noise (SNR) regimes. [J395]

"Improved BDFE Using A Priori Information for Turbo Equalization"

Turbo equalization improves communication system performance by iteratively exchanging information between soft-input soft-output (SISO) equalizer and SISO channel decoder. The trellis-based maximum a posteriori probability (MAP) algorithm serves as the optimum SISO equalizer for turbo equalization. However, MAP algorithm is unsuitable for systems with large modulation constellation size and severe inter-symbol interference (ISI) due to its prohibitively high computational complexity. In this paper, an improved SISO block decision feedback equalizer (BDFE) is proposed for low complexity turbo equalization. Unlike other sub-optimum equalizers which perform symbol by symbol detection, the proposed equalizer generates the soft output for each data bit by collecting information from a sequence of samples as in MAP algorithm. The sequence-based equalization is enabled by using not only soft a priori input from channel decoder, but also hard a priori information obtained from BDFE in previous iteration. The combination of soft a priori information and hard a priori information renders better performance with less iterations compared to other sub-optimum algorithms. In addition, the computational complexity of the proposed algorithm is on the same order as conventional SISO BDFE algorithm, and is much lower compared to the trellis-based MAP algorithm. [J396]

"Face-Based Digital Signatures for Video Retrieval"

The characterization of a video segment by a digital signature is a fundamental task in video processing. It is necessary for video indexing and retrieval, copyright protection, and other tasks. Semantic video signatures are those that are based on high-level content information rather than on low-level features of the video stream. The major advantage of such signatures is that they are highly invariant to nearly all types of distortion. A major semantic feature of a video is the appearance of specific persons in specific video frames. Because of the great amount of research that has been performed on the subject of face detection and recognition, the extraction of such information is generally tractable, or will be in the near future. We have developed a method that uses the pre-extracted output of face detection and recognition to perform fast semantic query-by-example retrieval of video segments. We also give the results of the experimental evaluation of our method on a database of real video. One advantage of our approach is that the evaluation of similarity is convolution-based, and is thus resistant to perturbations in the signature and independent of the exact boundaries of the query segment. [J397]

"An H.264/AVC Video Coder Based on a Multiple Description Scalar Quantizer"

Transmission of encoded video sequences over unreliable networks usually requires the adoption of protection techniques to guarantee good reconstruction quality at the receiver side. Multiple description coding (MDC) strategies add reliability to real-time video applications, where retransmission is not possible and packet losses afflict several frames degrading the overall quality. This paper presents a novel MDC scheme based on the H.264/AVC standard and a multiple description scalar quantizer which encodes the residual information into two descriptions. Finally, objective and visual performances are presented. [J398]

"A Novel Look-Up Table Design Method for Data Hiding With Reduced Distortion"

Look-up table (LUT)-based data hiding is a simple and efficient technique to hide secondary information (watermark) into multimedia work for various applications such as copyright protection, transaction tracking or content annotation. This paper studies the distortion introduced by a general LUT-based data hiding. We find that designing LUT according to the distribution of host data and watermark data can greatly reduce the distortion of LUT embedding. A new practical reduced-distortion LUT design method is developed for robust data hiding. The new method is applied in a wavelet domain image data hiding system and only significant wavelet coefficients are used to embed the watermark. A Gaussian mixture model and a related expectation-maximization algorithm-based method are employed to model the statistical distribution of the host image. The statistical model is used to select significant coefficients of the host image for data hiding. The experimental results show that compared to the conventional odd-even LUT embedding method, the presented new LUT data hiding algorithm provides average 1. 5-2. 5 dB PSNR improvement and better robustness for image watermarking. [J399]

"Anonymous Geo-Forwarding in MANETs through Location Cloaking"

In this paper, we address the problem of destination anonymity for applications in mobile ad hoc networks where geographic information is ready for use in both ad hoc routing and Internet services. Geographic forwarding becomes a lightweight routing protocol in favor of the scenarios. Traditionally the anonymity of an entity of interest can be achieved by hiding it among a group of other entities with similar characteristics, i.e., an anonymity set. In mobile ad hoc networks, generating and maintaining an anonymity set for any ad hoc node is challenging because of the node mobility, consequently the dynamic network topology. We propose protocols

that use the destination position to generate a geographic area called an anonymity zone (AZ). A packet for a destination is delivered to all the nodes in the AZ, which make up the anonymity set. The size of the anonymity set may decrease because nodes are mobile, yet the corresponding anonymity set management is simple. We design techniques to further improve node anonymity and reduce communication overhead. We use analysis and extensive simulation to study the node anonymity and routing performance, and to determine the parameters that most impact the anonymity level that can be achieved by our protocol. [J400]

"Securing Information Transfer in Distributed Computing Environments"

The problem of migrating sensitive information between systems in dynamic environments is increasingly important as distributed computing expands. A proposed policy-based approach provides controlled and secure transfer of user credentials and data across platforms. We propose a policy-driven data-protection system to address the inadequacies of current technological solutions in preserving the confidentiality and privacy of data while it migrates between platforms. More specifically, we describe our solution for securing credential migration that we're developing for productization. [J401]

"News Briefs"

Here we offer highlights of what's relevant in IT news. [J402]

"Modeling and detection of transformer internal incipient fault during impulse test"

Incipient faults are low magnitude and fast decaying transients, lasting only for a few microseconds during impulse tests of transformers. They are very difficult to detect, even for experts, and may cause severe problems leading to faults and consequent outage. Thus, simulation and diagnosis of incipient faults is very important requiring a valid model and advanced detection technique. In this paper, a new arc discharge model is proposed to simulate arcing phenomena between two discs of a power transformer winding, as one type of important incipient fault, during impulse test. Using wavelet transform techniques, a new methodology is developed. It is shown that winding input current, affected by arcing phenomena and obtained through impulse voltage test, provides important information for detection and analysis of this transient type of minor fault. A number of experiments and simulations were performed to evaluate the validity and accuracy of proposed model and diagnostic technique. [J403]

"Grid Computing Security: A Taxonomy"

Grid computing helps us overcome heterogeneity in terms of computing elements, operating systems, policy decisions, and environments. However, security issues impede us from adopting the grid as a widespread IT virtualization solution, so we must develop solutions to address these issues. [J404]

"A Simulation Tool to Predict the Impact of Soil Topologies on Coupling Between a Light Rail System and Buried Third-Party Infrastructure"

The production of stray currents by DC light rail systems leads to the corrosion of the supporting and third-party infrastructure in close proximity to the rail system. This paper simulates two parallel tracks that are occupied by two trains: one on each track. This type of modeling constitutes a case study that is utilized to investigate the effect of soil topologies on the corrosion performance of a floating DC light rail system focusing on the supporting and third-party infrastructure. The modeling technique used involves the accurate computation of the shunt and series parameters for use in a resistive-type model using a commercially available software package. The results demonstrate the importance that soil resistivity has on the corrosion risk to traction system and third-party infrastructure. Such information could ultimately be used to vary the level of stray current protection across a light rail system to ensure a consistent lifetime across the whole system. [J405]

"Analyzing Regulatory Rules for Privacy and Security Requirements"

Information practices that use personal, financial, and health-related information are governed by US laws and regulations to prevent unauthorized use and disclosure. To ensure compliance under the law, the security and privacy requirements of relevant software systems must properly be aligned with these regulations. However, these regulations describe stakeholder rules, called rights and obligations, in complex and sometimes ambiguous legal language. These "rules" are often precursors to software requirements that must undergo considerable refinement and analysis before they become implementable. To support the software engineering effort to derive security requirements from regulations, we present a methodology for directly extracting access rights and obligations from regulation texts. The methodology provides statement-level coverage for an entire regulatory document to consistently identify and infer six types of data access constraints, handle complex cross

references, resolve ambiguities, and assign required priorities between access rights and obligations to avoid unlawful information disclosures. We present results from applying this methodology to the entire regulation text of the US Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. [J406]

"Transformer Differential Protection Using Principal Component Analysis"

This paper describe a new algorithm for transformer differential protection, based on pattern recognition of the differential current obtained as the phasor sum of the current-transformer secondary currents. The algorithm uses principal component analysis to preprocess data from the power system in order to eliminate redundant information and enhance hidden pattern in differential current to discriminate between internal faults (transformer differential protection zone) from inrush and overexcitation conditions. The algorithm was proven using PSCAD/EMTDC simulations in a three-phase power system considering critical fault cases. The results show the feasibility to implement this algorithm for transformer differential protection. [J407]

"Tracing Worm Break-In and Contaminations via Process Coloring: A Provenance-Preserving Approach"

To detect and investigate self-propagating worm attacks against networked servers, the following capabilities are desirable: 1) raising timely alerts to trigger a worm investigation, 2) determining the break-in point of a worm, i.e., the vulnerable service from which the worm infiltrates the victim, and 3) identifying all contaminations inflicted by the worm during its residence in the victim. In this paper, we argue that the worm break-in provenance information has not been exploited in achieving these capabilities and thus propose process coloring, a new approach that preserves worm break-in provenance information and propagates it along operating- system-level information flows. More specifically, process coloring assigns a "color," a unique systemwide identifier, to each remotely accessible server process. The color will be either inherited by spawned child processes or diffused transitively through process actions. Process coloring achieves three new capabilities: color-based worm warning generation, break-in point identification, and log file partitioning. The virtualization-based implementation enables more tamper-resistant log collection, storage, and real-time monitoring. Beyond the overhead introduced by virtualization, process coloring only incurs very small additional system overhead. Experiments with real-world worms demonstrate the advantages of processing coloring over non-provenance-preserving tools. [J408]

"Detecting VoIP Floods Using the Hellinger Distance"

Voice over IP (VoIP), also known as Internet telephony, is gaining market share rapidly and now competes favorably as one of the visible applications of the Internet. Nevertheless, being an application running over the TCP/IP suite, it is susceptible to flooding attacks. If flooded, as a time-sensitive service, VoIP may show noticeable service degradation and even encounter sudden service disruptions. Because multiple protocols are involved in a VoIP service and most of them are susceptible to flooding, an effective solution must be able to detect and overcome hybrid floods. As a solution, we offer the VoIP flooding detection system (vFDS)-an online statistical anomaly detection framework that generates alerts based on abnormal variations in a selected hybrid collection of traffic flows. It does so by viewing collections of related packet streams as evolving probability distributions and measuring abnormal variations in their relationships based on the Hellinger distance-a measure of variability between two probability distributions. Experimental results show that vFDS is fast and accurate in detecting flooding attacks, without noticeably increasing call setup times or introducing jitter into the voice streams. [J409]

"Ultrasaturation Phenomenon in Power Transformers-Myths and Reality"

In this paper, the ultrasaturation phenomenon of power transformers during their energization is studied. It is shown that under special conditions, the currents observed after transformer switching on do not contain enough restraining information (e.g., second harmonic), which may lead to protection maloperation. This paper concentrates on a thorough explanation of the problem and possible causes of ultrasaturation. Theoretical investigations are supported and illustrated with simulation studies performed both with MATLAB and electromagnetic transients program-alternative transients program. The outcomes of this research can further be used as hints for substation operation personnel as well as for the development of new protection stabilization criteria, which is not discussed further in this paper. [J410]

"Modeling and Protection of Hexagonal Phase-Shifting Transformers-Part II: Protection"

Owing to several advantages over traditional phase shifters, applications of hexagonal phase-shifting transformers (PSTs) keep expanding. These transformers are built with unique connections of their windings, neither delta nor wye. Modeling and protection methods are not yet fully established for hexagonal phase shifters. This work is divided in two parts. In Part I, a digital model of a hexagonal PST has been developed and

validated. This part presents protection techniques for hexagonal PSTs. Several novel protection schemes have been developed based on ampere-turn balance equations of a hexagonal PST. These schemes include linear and nonlinear current-based protection methods, a power-based technique, and a phase comparison method. Protection schemes that require position of the tap changer for maximum sensitivity as well as a method to work without this extra information are presented. The developed techniques have been validated with digital and physical made-to-scale transformer models, and implemented on a general-purpose microprocessor-based relay platform. This material is of value to protection engineers facing the problem of protecting hexagonal PSTs. [J411]

"Multipath Key Establishment for Wireless Sensor Networks Using Just-Enough Redundancy Transmission"

In random key predistribution techniques for wireless sensor networks, a relatively small number of keys are randomly chosen from a large key pool and are loaded on the sensors prior to deployment. After deployment, each sensor tries finding a common key shared by itself and each of its neighbors to establish a link key to protect the wireless communication between themselves. One intrinsic disadvantage of such techniques is that some neighboring sensors do not share any common key. In order to establish a link key among these neighbors, a multihop secure path may be used to deliver the secret. Unfortunately, the possibility of sensors being compromised on the path may render such an establishment process insecure. In this work, we propose and analyze the just-enough redundancy transmission (JERT) scheme that uses the powerful maximum-distance separable (MDS) codes to address the problem. In the JERT scheme, the secret link key is encoded in (n, k) MDS code and transmitted through multiple multihop paths. To reduce the total information that needs to be transmitted, the redundant symbols of the MDS codes are transmitted only if the destination fails to decode the secret. The JERT scheme is demonstrated to be efficient and resilient against node capture. One salient feature of the JERT scheme is its flexibility of trading transmission for lower information disclosure. [J412]

"SBK: A Self-Configuring Framework for Bootstrapping Keys in Sensor Networks"

Key pre-distribution has been claimed to be the only viable approach for establishing shared keys between neighboring sensors after deployment for a typical sensor network. However, none of the proposed key pre-distribution schemes simultaneously achieves good performance in terms of scalability in network size, key-sharing probability between neighboring sensors, memory overhead for keying information storage, and resilience against node capture attacks. In this paper, we propose SBK, an in-situ self-configuring framework to bootstrap keys in large-scale sensor networks. SBK is fundamentally different compared to all key pre-distribution schemes. It requires no keying information pre-deployment. In SBK, sensors differentiate their roles as either service nodes or worker nodes after deployment. Service sensors construct key spaces, and distribute keying information in order for worker sensors to bootstrap pairwise keys. An improved scheme, iSBK, is also proposed to speed up the bootstrapping procedure. We conduct both theoretical analysis and simulation study to evaluate the performances of SBK and iSBK. To the best of our knowledge, SBK and iSBK are the only key establishment protocols that simultaneously achieve good performance in scalability, key-sharing probability, storage overhead, and resilience against node capture attacks. [J413]

"TROP: A Novel Approximate Link-State Dissemination Framework For Dynamic Survivable Routing in MPLS Networks"

In this paper, a novel approximate link-state dissemination framework, called TROP, is proposed for shared backup path protection (SBPP) in multiprotocol label switching (MPLS) networks. While performing dynamic explicit survivable routing in a distributed environment, link-state dissemination may cause a nontrivial signaling overhead in the process of exploring spare resource sharing among individual backup label switched paths (LSPs). Several previously reported studies have tackled this problem by initiating a compromise between the amount of dissemination and the achievable extent of resource sharing. The paper first summarizes the previously reported schemes into a compact and general link-state dissemination framework by way of singular value decomposition (SVD). To improve the accuracy of the matrix reconstruction and to eliminate the overestimation of the sharable spare capacity along each link, a novel SVD approach based on the min-plus algebra (also called tropical semirings) is introduced. Simulation results show that the proposed schemes can achieve a lower blocking probability than that by all the other counterpart schemes while taking the same complexity of link-state dissemination. This great advantage is gained at the expense of a longer computation time for solving a linear program (LP) in each dissemination cycle at the core nodes. We also consider the stale link-state phenomena that may cause imprecision in the routing information at the ingress nodes due to the delay in the periodic/event-driven link-state update message advertisement. [J414]

"Security and Privacy for Distributed Multimedia Sensor Networks"

There is a critical need to provide privacy and security assurances for distributed multimedia sensor networking in applications including military surveillance and healthcare monitoring. Such guarantees enable the widespread adoption of such information systems, leading to large-scale societal benefit. To effectively address protection and reliability issues, secure communications and processing must be considered from system inception. Due to the emerging nature of broadband sensor systems, this provides fertile research ground for proposing more paradigm-shifting approaches. This paper discusses issues in designing for security and privacy in distributed multimedia sensor networks. We introduce the heterogeneous lightweight sensornets for trusted visual computing framework for distributed multimedia sensor networks. Protection issues within this architecture are analyzed, leading to the development of open research problems including secure routing in emerging free-space optical sensor networks and distributed privacy for vision-rich sensor networking. Proposed solutions to these problems are presented, demonstrating the necessary interaction among signal processing, networking, and cryptography. [J415]

"A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations"

The Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations are two crucial provisions in the protection of healthcare privacy. Privacy regulations create a principle to assure that patients have more control over their health information and set limits on the use and disclosure of health information. The security regulations stipulate the provisions implemented to guard data integrity, confidentiality, and availability. Undoubtedly, the cryptographic mechanisms are well defined to provide suitable solutions. In this paper, to comply with the HIPAA regulations, a flexible cryptographic key management solution is proposed to facilitate interoperations among the applied cryptographic mechanisms. In addition, case of consent exceptions intended to facilitate emergency applications and other possible exceptions can also be handled easily. [J416]

"Power-Efficient Direct-Voting Assurance for Data Fusion in Wireless Sensor Networks"

Wireless sensor networks place sensors into an area to collect data and send them back to a base station. Data fusion, in which collected data are fused before they are sent to the base station, is usually implemented over the network. Since a sensor is typically placed in locations that are accessible to malicious attackers, information assurance of the data fusion process is very important. A witness-based approach by Du, W, et al (2003) has been proposed to verify the fusion data. In this approach, the base station receives the fusion data and "votes" on the data from a randomly chosen sensor node. The vote comes from other sensor nodes, called "witnesses," to confirm the correctness of the fusion data. Since the base station receives the vote through the chosen node, this node could forge the vote if it is compromised. Accordingly, the witness node must apply cryptographic operations to the vote to prevent this forgery. The cryptographic operation requires more bits than the vote, increasing the transmission burden from the chosen node to the base station. The chosen node consumes too much power. This work improves the witness-based approach using a direct voting mechanism such that the proposed scheme performs better in terms of assurance, overhead, and delay. The witness node transmits the vote directly to the base station. Forgery does not pose a problem in this scheme. Moreover, fewer bits are necessary to represent the vote, significantly reducing the power consumption. Performance analysis and simulation results indicate that the proposed approach has a 40-times lower overhead than the witness-based approach. [J417]

"Controlling IP Spoofing through Interdomain Packet Filters"

The distributed denial-of-service (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper, we propose an interdomain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in border gateway protocol (BGP) route updates and are deployed in network border routers. We establish the conditions under which the IDPF framework correctly works in that it does not discard packets with valid source addresses. Based on extensive simulation studies, we show that, even with partial deployment on the Internet, IDPFs can proactively limit the spoofing capability of attackers. In addition, they can help localize the origin of an attack packet to a small number of candidate networks. [J418]

"Efficient Remote Data Possession Checking in Critical Information Infrastructures"

Checking data possession in networked information systems such as those related to critical infrastructures (power facilities, airports, data vaults, defense systems, etc.) is a matter of crucial importance. Remote data

possession checking protocols permit to check that a remote server can access an uncorrupted file in such a way that the verifier does not need to know beforehand the entire file that is being verified. Unfortunately, current protocols only allow a limited number of successive verifications or are impractical from the computational point of view. In this paper, we present a new remote data possession checking protocol such that: 1) it allows an unlimited number of file integrity verifications; 2) its maximum running time can be chosen at set-up time and traded off against storage at the verifier. [J419]

"Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms"

Continued advances in mobile networks and positioning technologies have created a strong market push for location-based applications. Examples include location-aware emergency response, location-based advertisement, and location-based entertainment. An important challenge in the wide deployment of location-based services (LBSs) is the privacy-aware management of location information, providing safeguards for location privacy of mobile clients against vulnerabilities for abuse. This paper describes a scalable architecture for protecting the location privacy from various privacy threats resulting from uncontrolled usage of LBSs. This architecture includes the development of a personalized location anonymization model and a suite of location perturbation algorithms. A unique characteristic of our location privacy architecture is the use of a flexible privacy personalization framework to support location k-anonymity for a wide range of mobile clients with context-sensitive privacy requirements. This framework enables each mobile client to specify the minimum level of anonymity that it desires and the maximum temporal and spatial tolerances that it is willing to accept when requesting k-anonymity-preserving LBSs. We devise an efficient message perturbation engine to implement the proposed location privacy framework. The prototype that we develop is designed to be run by the anonymity server on a trusted platform and performs location anonymization on LBS request messages of mobile clients such as identity removal and spatio-temporal cloaking of the location information. We study the effectiveness of our location cloaking algorithms under various conditions by using realistic location data that is synthetically generated from real road maps and traffic volume data. Our experiments show that the personalized location k-anonymity model, together with our location perturbation engine, can achieve high resilience to location privacy threats without introducing any significant--performance penalty. [J420]

"Privacy Protection Against Malicious Adversaries in Distributed Information Sharing Systems"

We address issues related to sharing information in a distributed system consisting of autonomous entities, each of which holds a private database. We consider threats from malicious adversaries that can deviate from the designated protocol and change their input databases. We classify malicious adversaries into two widely existing subclasses, namely weakly and strongly malicious adversaries, and propose protocols that can effectively and efficiently protect privacy against malicious adversaries. [J421]

"Protection of Database Security via Collaborative Inference Detection"

Malicious users can exploit the correlation among data to infer sensitive information from a series of seemingly innocuous data accesses. Thus, we develop an inference violation detection system to protect sensitive data content. Based on data dependency, database schema and semantic knowledge, we constructed a semantic inference model (SIM) that represents the possible inference channels from any attribute to the pre-assigned sensitive attributes. The SIM is then instantiated to a semantic inference graph (SIG) for query-time inference violation detection. For a single user case, when a user poses a query, the detection system will examine his/her past query log and calculate the probability of inferring sensitive information. The query request will be denied if the inference probability exceeds the prespecified threshold. For multi-user cases, the users may share their query answers to increase the inference probability. Therefore, we develop a model to evaluate collaborative inference based on the query sequences of collaborators and their task-sensitive collaboration levels. Experimental studies reveal that information authoritativeness, communication fidelity and honesty in collaboration are three key factors that affect the level of achievable collaboration. An example is given to illustrate the use of the proposed technique to prevent multiple collaborative users from deriving sensitive information via inference. [J422]

"Testing a Collaborative DDoS Defense In a Red Team/Blue Team Exercise"

Testing security systems is challenging because a system's authors have to play the double role of attackers and defenders. Red team/blue team exercises are an invaluable mechanism for security testing. They partition researchers into two competing teams of attackers and defenders, enabling them to create challenging and realistic test scenarios. While such exercises provide valuable insight into vulnerabilities of security systems, they are very expensive and thus rarely performed. In this paper we describe a red team/blue team exercise, sponsored by DARPA's FTN program, and performed October 2002 --- May 2003. The goal of the exercise was

to evaluate a collaborative DDoS defense, comprised of a distributed system, COSSACK, and a stand-alone defense, D-WARD. The role of the blue team was played by developers of the tested systems from USC/ISI and UCLA, the red team included researchers from Sandia National Laboratory, and all the coordination, experiment execution, result collection and analysis was performed by the white team from BBN Technologies. This exercise was of immense value to all involved --- it uncovered significant vulnerabilities in tested systems, pointed out desirable characteristics in DDoS defense systems (e.g., avoiding reliance on timing mechanisms), and taught us many lessons about testing of DDoS defenses. [J423]

"Medical Record Privacy and Security in a Digital Environment"

Quality healthcare increasingly means addressing the security, privacy, and confidentiality of medical records in both wire-line and wireless environments. This article attempts to address these concerns by presenting a comparison of data-flow patterns in an electronic healthcare setting to those in traditional medical offices and demonstrating cost-effective ways that IT consultants can help healthcare providers working in EHRs maintain and administer their own privacy and security policies. [J424]

"Securing wireless sensor networks against aggregator compromises"

A common approach to overcome the limited nature of sensor networks is to aggregate data at intermediate nodes. A challenging issue in this context is to guarantee end-to-end security mainly because sensor networks are extremely vulnerable to node compromises. We propose three schemes to secure data aggregation that rely on multipath routing. The first guarantees data confidentiality through secret sharing, while the second and third provide data availability through information dispersal. Based on qualitative analysis and implementation, we show that by applying these schemes, a sensor network can achieve data confidentiality, authenticity, and protection against denial of service attacks even in the presence of multiple compromised nodes. [J425]

"Detecting and avoiding wormhole attacks in wireless ad hoc networks"

A particularly severe attack on routing protocols in ad hoc networks is the so-called worm- hole attack in which two or more colluding attackers record packets at one location, and tunnel them to another location for replay at that remote location. When this attack targets specifically routing control packets, the nodes that are close to the attackers are shielded from any alternative routes with more than one or two hops to the remote location. All routes are thus directed to the wormhole established by the attackers. In the optimized link state routing protocol, if a wormhole attack is launched during the propagation of link state packets, the wrong link information percolates throughout the network, leading to routing disruption. In this article we devise an efficient method to detect and avoid wormhole attacks in the OLSR protocOLSR protocolol. This method first attempts to pinpoint links that may potentially be part of a wormhole tunnel. Then a proper wormhole detection mechanism is applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbors (endpoints of the wormhole). The proposed solution exhibits several advantages, among which are its nonreliance on any time synchronization or location information, and its high detection rate under various scenarios. [J426]

"Experiences with Electronic Health Records"

The healthcare system in Denmark is well known for its high level of IT support and interoperability. The Danish healthcare system integrates several central technological solutions across hospital information and electronic medical record systems throughout Denmark. Important business drivers for this high level of interoperability include unique citizen ID numbers and a publicly funded healthcare system in which hospital reimbursements are based on electronic submissions of diagnosis and procedure codes to a central register. [J427]

"Local fidelity, constrained codes, and the Meru Prastara"

Information theory provides fundamental bounds on the tradeoff between achievable distortion in communication and the amount of resources that are allocated to the communication system. For optimal point-to-point communication, this is a condition on rate matching. Most theoretical computation work has focused on single-letter fidelity and resource criteria due to tractability. However, these may not reflect true system objectives and constraints. So, it is desirable to extend analysis to non-single-letter fidelity and resource criteria. In certain cases, the problem can be reduced to combinatorics and becomes tractable. [J428]

"Chattering Free Robust Control for Nonlinear Systems"

A new design method fully using the sliding manifold information is proposed to achieve a chattering free nonlinear robust control law. Guaranteed asymptotic stability is proven using the Lyapunov second theorem and

the invariance principle. An explicit time varying feedback gain derived according to the global stability and sliding manifold variations is proven to be uniquely solvable based on the Perron-Frobenius theorem. The proposed nonlinear controller, which relies on the nominal system only, has the following advantages: 1) it maintains the benefits of the variable structure control which drives the system along a specified sliding surface with guaranteed stability under the bounded functional and parametric uncertainties, as well as drives the system reaching the sliding manifold in a finite time; 2) the proposed controller which eliminates the discontinuity does not induce chattering as in the variable structure control; and 3) theoretical and numerical studies in this paper show that the proposed control methodology is superior to traditional variable structure controls in terms of smooth transient performance and saturation protection for the large initial gain. [J429]

"Minimizing information leakage in the DNS"

The domain name system is the global lookup service for network resources. To protect DNS information, the DNS security extensions have been developed and deployed on branches of the DNS to provide authentication and integrity protection using digital signatures. However, signed DNS nodes were found to have an unfortunate side effect: an attacker can query them as reconnaissance before attacking hosts on a particular network. There are different ways a zone administrator can minimize information leakage and still take advantage of DNSSEC for integrity and source authentication. This article describes the risk and examines the protocol and operational options and looks at their advantages and drawbacks. [J430]

"Public Key Broadcast Encryption Schemes With Shorter Transmissions"

Broadcast encryption allows a sender to securely distribute messages to a dynamically changing set of users over an insecure channel. In a public key broadcast encryption (PKBE) scheme, this encryption is performed in the public key setting, where the public key is stored in a user's device, or directly transmitted to the receivers along with ciphertexts. In this paper, we propose two PKBE schemes for stateless receivers which are transmission-efficient. A distinctive feature in our first construction is that, different than existing schemes in the literature, only a fraction of the public key related to the set of intended receivers is required in the decryption process. This feature results in the first PKBE scheme with O(r) transmission cost and O(1) user storage cost for r revoked users. Our second construction is a generalized version of the first one providing a tradeoff between ciphertext size and public key size. With appropriate parametrization, we obtain a PKBE scheme with (Oradicn) transmission cost and O(1) user storage cost for any large set of n users. The transmission cost of our second scheme is at least 30% less than that of the recent result of Boneh et al.'s PKBE scheme, which is considered as being the current state-of-the-art. By combining the two proposed schemes, we suggest a PKBE scheme that achieves further shortened transmissions, while still maintaining O(1) user storage cost. The proposed schemes are secure against any number of colluders and do not require costly re-keying procedures followed by revocation of users. [J431]

"Evaluation of Breakdown Characteristics of Gas Insulated Switchgears for Non-Standard Lightning Impulse Waveforms-Breakdown Characteristics for Non-Standard Lightning Impulse Waveforms Associated with Lightning Surges"

To lower the insulation specifications (specifically, the lightning impulse withstand voltage) of a gas insulated switchgear (GIS) and thus cut the equipment cost while maintaining the high reliability of its insulation performance, it is necessary to define in an organized way the insulation characteristics for non-standard lightning impulse voltage waveforms that represent actual surge waveforms in the field and compare them with the characteristics for the standard lightning impulse waveform quantitatively. In the preceding paper, lightning surge waveforms and disconnector switching surge waveforms at UHV, 500 kV, and 275 kV substations were analyzed and five to six non-standard lightning surge waveforms with basic frequencies of 0.6 to 5.0 MHz were identified. In this paper, the dielectric breakdown voltage-time characteristics were measured under several different conditions mainly for the quasi-uniform SF6gas gaps that represent an insulation element of a GIS toward four kinds of non-standard lightning impulse waveforms associated with lightning surges. As a result, in the tested range, the dielectric breakdown values for nonstandard lightning impulse waveforms were higher than for the standard lightning impulse waveform by 3% to 32%. [J432]

"Identity Management, Privacy, and Price Discrimination"

In economics, privacy is usually discussed in the context of consumer preferences and price discrimination. But what forms of personal data privacy are compatible with merchants' interests in knowing more about their consumers, and how can identity management systems protect information privacy while enabling personalization and price discrimination? [J433]

"Privacy and Identity Management"

Creating and managing individual identities is a central challenge of the digital age. As identity management systems defined here as programs or frameworks that administer the collection, authentication, or use of identity and information linked to identity are implemented in both the public and private sectors, individuals are required to identify themselves with increasing frequency. Traditional identity management systems are run by organizations that control all mechanisms for authentication (establishing confidence in an identity claim's truth) and authorization (deciding what an individual should be allowed to do), as well as any behind-the-scenes profiling or scoring of individuals. Recent work has looked toward more user-centric models that attempt to put individuals in charge of when, where, how, and to whom they disclose their personal information. [J434]

"Inference of Security Hazards from Event Composition Based on Incomplete or Uncertain Information"

In many security-related contexts, a quick recognition of security hazards is required. Such recognition is challenging, since available information sources are often insufficient to infer the occurrence of hazards with certainty. This requires that the recognition of security hazard is carried out using inference based on patterns of occurrences distributed over space and time. The two main existing approaches to the inference of security hazards are a) custom-coded solutions, which are tailored to specific patterns, and cannot respond quickly to changes in the patterns of occurrences used for inference, and b) approaches based on direct statistical inferencing techniques, such as regression, which do not enable combining various kinds of evidence regarding the same hazard. In this work, we introduce a more generic formal framework which overcomes the aforementioned deficiencies, together with a case study illustrating the detection of DoS attacks. [J435]

"The Hidden Difficulties of Watching and Rebuilding Networks"

The subtleties of network protection can bedevil even experienced IT staff and security researchers. In this installment of secure systems, we focus on two areas of network defense that are particularly troublesome to manage: network intrusion recovery and ubiquitous network monitoring. [J436]

"Sharp Figures, Fuzzy Purpose"

Simson Garfinkel reviews Security Data Visualization: Graphical Techniques for Network Analysis by Greg Conti. [J437]

"The Mobile Sensing Platform: An Embedded Activity Recognition System"

Activity-aware systems have inspired novel user interfaces and new applications in smart environments, surveillance, emergency response, and military missions. Systems that recognize human activities from body-worn sensors can further open the door to a world of healthcare applications, such as fitness monitoring, eldercare support, long-term preventive and chronic care, and cognitive assistance. Wearable systems have the advantage of being with the user continuously. So, for example, a fitness application could use real-time activity information to encourage users to perform opportunistic activities. Furthermore, the general public is more likely to accept such activity recognition systems because they are usually easy to turn off or remove. [J438]

"Fiber-Optics-Based Fault Detection in Power Systems"

A fiber-optics-based sensing network applicable for fault detection in power system is presented. The proposed scheme is secure and immune from interferences. At each monitoring location, passive rugged fiber-Bragg-grating-based sensors are deployed. They use fast and compact magnetostrictive transducers instead of current or potential transformers to translate current-induced magnetic field into optical signal. These sensors can be compensated for temperature drift and easily be integrated into an optical sensing network. A broadband light source at a substation scans the change in reflected optical power at a unique frequency band that corresponds to the surge in magnetic field associated with an increased fault current at a certain location. A unique feature of this real-time scheme is that it only requires current information for fault detections in both radial and networked systems with various pole structures and line configurations. It can easily coordinate with other protective devices and is free from any time-current coordination curves. The proposed scheme has been extensively tested by simulations. They confirm that the proposed scheme is able to detect the faults irrespective of the type and location. It also performs well in presence of harmonics, high impedance, and sensors malfunctions, as well as sensor noise. [J439]

"Accelerating Real-Time String Searching with Multicore Processors"

String searching is at the core of tools used to search, filter, and protect data, but this has become increasingly difficult to do in real time as communication speed grows. The authors present an optimization strategy for a popular algorithm that fully exploits the IBM cell broadband engine architecture to perform exact string matching against large dictionaries and also offer various solutions to alleviate memory congestion. [J440]

"Identifying the Primary Fault Section After Contingencies in Bulk Power Systems"

This paper deals with the problem of fault section estimation in electric power systems, undertaken at a control center level and using information about the operation of protection relays and circuit breakers. The developed methodology should be used after the occurrence of contingencies with definitive disconnections, and before beginning the process of network restoration. Due to the absence of an analytic formulation, the problem calls for the use of artificial-intelligence techniques, such as neural networks and expert systems. Neural networks are employed to model the protection systems, dealing with the uncertainties involved with relay and circuit-breaker operation messages. An expert system is used to complement the results provided by the neural networks, considering the network topology. The results show that the developed methodology is applicable to real large-scale power systems. In addition, it is capable of noise suppression in relay and circuit-breaker trip messages, treats multiple faults naturally, and infers a solution even in cases when remote backup protection action occurs. [J441]

"Reviews of [J("Security for Mobile Networks and Platforms", Aissi, S., et al) and (Cooperation in Wireless Networks: Principles and Applications, Fitzek, H.P. and Katz, M.D., Eds.; 2006)]"

Two books are reviewed in this column: Security for Mobile Networks and Platforms (S. Aissi et al.; 2006) and Cooperation in Wireless Networks: Principles and Applications (H.P. Fitzek and M.D. Katz, Eds.; 2006). [J442]

"Multimedia Retrieval and Delivery: Essential Metadata Challenges and Standards"

Multimedia information retrieval (MIR) and delivery plays an important role in many application domains due to the increasing need to identify, filter, and manage growing amounts of data, notably multimedia information. To efficiently manage and exchange multimedia information, interoperability between coded data and metadata is required and standardization is central to achieving the necessary level of interoperability. In the context of this paper, the term retrieval refers to the process by which a user, human or machine, identifies the content it needs, and the term delivery refers to the adaptive transport and consumption of the identified content in a particular context or usage environment. Both the retrieval and delivery processes may require content and context metadata. This paper will argue that maximum quality of experience depends not only on the content itself (and thus content metadata) but also on the consumption conditions (thus context metadata). Additionally, the rights and protection conditions have become critically important in recent years, especially with the explosion of electronic music commerce and different ldquoshoppingrdquo conditions. This paper will review existing multimedia standards related to information retrieval and adaptive delivery of multimedia content, emphasizing the need for such standards, and will show how these standards can help the development, dissemination, and valorization of MIR research results. Moreover, it will also discuss limitations of the current standards and anticipate what future standardization activities are relevant and needed. Due to space limitations, the paper will mainly concentrate on MPEG standards although many other relevant standards are also reviewed and discussed. [J443]

"Is Anybody Home?"

At the recent consumer electronics show CES the big story was about how all the devices we'll be buying in the very near future will be Internet-capable. We should think about the broader notion of an ecology of connected devices: why this notion didn't work in the past, what it'll take to make it work this time, and what issues we, as designers of this ecology, should be thinking about as we move toward the future. [J444]

"Bandwidth Guaranteed Routing With Fast Restoration Against Link and Node Failures"

An important feature of MPLS networks is local restoration where detour paths are set-up a priori. The detour is such that failed links or nodes can be bypassed locally from the first node that is upstream from the failures. This local bypass activation from the first detection point for failures permits much faster recovery than end-to-end path based mechanisms that require failure information to propagate to the network edges. However, local restoration of bandwidth guaranteed connections can be expensive in the additional network capacity needed. Hence, it is important to minimize and share restoration capacity. The problem of routing with local restoration requirements has been studied previously in a dynamic on-line setting. However, there are no satisfactory algorithms for the problem of pre-provisioning fast restorable connections when the aggregate traffic demands are known (as would be the case when a set of routers are to be interconnected over an optical network or for

pre-provisioned ATM over MPLS overlays). The contribution of this paper is a fast combinatorial approximation algorithm for maximizing throughput when the routed traffic is required to be locally restorable. To the best of our knowledge, this is the first combinatorial algorithm for the problem with a performance guarantee. Our algorithm is a fully polynomial time approximation scheme (FPTAS), i.e., for any given epsiv > 0, it guarantees (1+epsiv)-factor closeness to the optimal solution, and runs in time polynomial in the network size and [1/(epsiv)]. We compare the throughput of locally restorable routing with that of unprotected routing and 1+1-dedicated path protection on actual US/European ISP topologies taken from the Rocketfuel project . [J445]

"Distributed source coding using short to moderate length rate-compatible LDPC codes: the entire Slepian-Wolf rate region"

In this paper, we propose a scheme for distributed source coding of correlated sources using a single systematic LDPC code. In particular, since we are interested in wireless sensor network applications, we consider LDPC codes with short to moderate lengths that achieve every arbitrary coding rate on the Slepian-Wolf rate region. We simplify the distributed source coding problem to the rate-compatible LDPC code design with an unequal error protection property. The decoders communicate to each other to exchange information bits prior to decoding. However, thereafter, each performs the decoding independently. Therefore, errors in one decoder do not affect the other one. The simulation results confirm that the gap from the theoretical limit remains almost the same for different rates on the Slepian-Wolf rate region. First, we consider two correlated sources. We show that our proposed scheme improves the performance of distributed source coding of two sources considerably. This benefit is more stressed for application with short to moderate length sequences. Then, we study distributed source coding of three sources. As a special case, we investigate three sources that are pairwise correlated with the same correlation probability. We show that the gap from the theoretical limit is smaller than that of previous work. We also investigate the distributed source coding of correlated sources when there is no prior knowledge of the correlation parameter at the time of code design. We note that although the proposed distributed source coding is well suited for sensor networks (where sequences with less than 10000 bits are used), the method can be generalized to other distributed source coding applications. [J446]

"On Minimax Optimal Linear Transforms for Detection with Side Information in Gaussian Setup"

We consider the problem of detection with side information to model robust signal hashing for content tracking. The receiver observes corrupted (by additive colored Gaussian noise) message signals and performs detection, knowing the noise statistics and only some partial information about the message set, which is obtained via applying a dimensionality- reducing linear transform (represented by a full-rank matrix) to the messages. We derive the optimal GLRT-rule for the binary detection setup and find the corresponding error probability. Next, under some mild assumptions on the message set, we analytically derive the minimax-optimal linear transform matrix that minimizes the worst (over the set of messages) case error probability. [J447]

"Mobile Privacy in Wireless Networks-Revisited"

With the widespread use of mobile devices, the privacy of mobile location information becomes an important issue. In this paper, we present the requirements on protecting mobile privacy in wireless networks, and identify the privacy weakness of the third generation partnership project-authentication and key agreement (3GPP-AKA) by showing a practical attack to it. We then propose a scheme that meets these requirements, and this scheme does not introduce security vulnerability to the underlying authentication scheme. Another feature of the proposed scheme is that on each use of wireless channel, it uses a one-time alias to conceal the real identity of the mobile station with respect to both eavesdroppers and visited (honest or false) location registers. Moreover, the proposed scheme achieves this goal of identity concealment without sacrificing authentication efficiency. [J448]

"Efficient Distributed Bandwidth Management for MPLS Fast Reroute"

As service providers move more applications to their IP/MPLS (multiple protocol label switching) backbone networks, rapid restoration upon failure becomes more and more crucial. Recently MPLS fast reroute has attracted lots of attention as it was designed to meet the needs of real-time applications, such as voice over IP. MPLS fast reroute achieves rapid restoration by computing and signaling backup label switched path (LSP) tunnels in advance and re-directing traffic as close to failure point as possible. To provide a guarantee of bandwidth protection, extra bandwidth has to be reserved on backup paths. Using path merging technique as described in IETF RFC 4090 only, the network is able to share some bandwidth on common links among backup paths of the same service LSP, i.e., so-called intra-sharing. But no solution is provided on how to share bandwidth among backup paths of different service LSPs, i.e., so-called inter-sharing. In this paper, we provide an efficient distributed bandwidth management solution. This solution allows bandwidth sharing among backup

paths of the same and different service LSPs, i.e., both intra-sharing and inter-sharing, with a guarantee of bandwidth protection for any single node/link failure. We also propose an efficient algorithm for backup path selection with the associated signaling extensions for additional information distribution and collection. To evaluate our schemes, we compare them via simulation with the basic MPLS fast reroute proposal, IETF RFC 4090, on two networks. Our simulation results show that using our bandwidth management scheme can significantly reduce restoration overbuild from about 250% to about 100%, and our optimized backup path selection can further reduce restoration overbuild to about 60%. [J449]

"Toward an analytical approach to anonymous wireless networking"

Communications in a wireless network are susceptible to unauthorized traffic analysis by eavesdroppers. Although cryptography can protect the contents of communication, the transmission times of packets alone can reveal significant networking information such as source- destination pairs and routes of traffic flow. This article focuses on analytical approaches to anonymous networking for the prevention of information retrieval through packet timing analysis. In particular, an analytical measure for route anonymity is proposed using information theoretic equivocation. Based on the metric, provably anonymous countermeasures are described for wireless ad hoc and sensor networks, where traffic is subjected to strict constraints on medium access and latency. A key objective is to bridge a long standing gap between the information theoretic approach to secrecy in communication, and a more pragmatic approach of Chaum mixing used in anonymous systems on the Internet. The efficacy of the proposed approach is demonstrated using an orthogonal transmitter directed signaling network. [J450]

"Computationally Efficient PKI-Based Single Sign-On Protocol, PKASSO for Mobile Devices"

In an attempt to expand Public Key Infrastructure (PKI) usage to a ubiquitous and mobile computing environment, we found that the deployment of the PKI on a resource-constrained device such as an 8-bit microprocessor leads to user-obstructive latency or additional circuitry for the operations. To alleviate these limitations, we propose a new PKI-based authentication protocol and security infrastructure, namely, PKASSO, which is enhanced with the single sign-on and delegation technology that is used especially for mobile devices with restricted computation power. PKASSO offloads complex PKI operations from the mobile devices to the infrastructure so as to keep the hardware and software complexity of the devices as low as possible. In addition, even though a conventional delegation mechanism cannot support a nonrepudiation mechanism against malicious user behavior, PKASSO can provide such a mechanism by devising a referee server that, on one hand, generates binding information between a device and authentication messages and, on the other hand, retains the information in its local storage for future accusation. We present the detailed design and performance evaluation of PKASSO and offer a protocol analysis in terms of user authentication latency and the completeness of the protocol. According to the performance evaluation, the authentication latency of our infrastructure (which averages 0.082 second) is much shorter than the authentication latency of a conventional PKI-based authentication latency (which averages 5.01 seconds). [J451]

"High impedance fault detection in power distribution networks using time-frequency transform and probabilistic neural network"

An intelligent approach for high impedance fault (HIF) detection in power distribution feeders using advanced signal-processing techniques such as time-time and time-frequency transforms combined with neural network is presented. As the detection of HIFs is generally difficult by the conventional over-current relays, both time and frequency information are required to be extracted to detect and classify HIF from no fault (NF). In the proposed approach, S- and TT-transforms are used to extract time-frequency and time-time distributions of the HIF and NF signals, respectively. The features extracted using S- and TT-transforms are used to train and test the probabilistic neural network (PNN) for an accurate classification of HIF from NF. A qualitative comparison is made between the HIF classification results obtained from feed forward neural network and PNN with same features as inputs. As the combined signal-processing techniques and PNN take one cycle for HIF identification from the fault inception, the proposed approach was found to be the most suitable for HIF classification in power distribution networks with wide variations in operating conditions. [J452]

"Design Strategies for Load-Shedding Schemes Against Voltage Collapse in the Hellenic System"

Analytical description of the design of individual load-shedding schemes against voltage collapse in the Hellenic system is presented in this paper. Analysis and simulation results that validate the efficiency of these protection schemes are provided. This information may prove helpful for the design of similar load-shedding schemes in the future. Two event-driven load-shedding schemes based on design strategies proposed in this paper have been already implemented in the Hellenic system. [J453]

"Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key"

The two-party Diffie-Hellman (DH) key-exchanging technique is extended to generate (i) multiple two-party keys and (ii) one multi-party key. The participants in the former case exchange two public keys and generate 15 shared keys. Of these, 4 keys are called base keys, because they are used to generate the other 11 keys called extended keys. The main advantages are the reduction of the key exchange overhead, increase of additional protection to the keys and widening of applicability. In the latter case, an efficient contributory multi-party key-exchanging technique for a large static group is proposed. In this technique, a member who acts as a group controller forms two-party groups with other group members and generates a DH-style shared key per group. It then combines these keys into a single multi-party key and acts as a normal group member. The proposed technique has been compared with other multi-party key-generating techniques, and satisfactory results have been obtained. [J454]

"Privacy Ontology Support for E-Commerce"

Privacy is becoming increasingly important due to the advent of e-commerce. E-commerce applications frequently require customers to divulge many personal details about themselves that must be protected carefully in accordance with privacy principles and regulations. Here, the authors define a privacy ontology to support the provision of privacy and help derive the level of privacy associated with e-commerce transactions and applications. The privacy ontology provides a framework against which e-commerce sites can benchmark their privacy policies and implementations. [J455]

"Defense of trust management vulnerabilities in distributed networks"

Establishing trust among distributed network entities has been recognized as a powerful tool to secure distributed networks such as MANETs and sensor networks. Similar to most security schemes, trust establishment methods themselves can be vulnerable to attacks. In this article we investigate the benefits of introducing trust into distributed networks, the vulnerabilities in trust establishment methods, and the defense mechanisms. Five attacks against trust establishment methods are identified, and defense techniques are developed. Effectiveness of the attacks and the defense is demonstrated in the scenarios of securing routing protocols and detecting malicious nodes in MANETs. [J456]

"Achievable Error Exponents for the Private Fingerprinting Game"

Fingerprinting systems in the presence of collusive attacks are analyzed as a game between a fingerprinter and a decoder on the one hand, and a coalition of two or more attackers on the other hand. The fingerprinter distributes, to different users, different fingerprinted copies of a host data (covertext), drawn from a memoryless stationary source, embedded with different fingerprints. The coalition members create a forgery of the data while aiming at erasing the fingerprints in order not to be detected. Their action is modeled by a multiple-access channel (MAC). We analyze the performance of two classes of decoders, associated with different kinds of error events. The decoder of the first class aims at detecting the entire coalition, whereas the second is satisfied with the detection of at least one member of the coalition. Both decoders have access to the original covertext data and observe the forgery in order to identify member(s) of the coalition. Motivated by a worst case approach, we assume that the coalition of attackers is informed of the hiding strategy taken by the fingerprinter and the decoder, while they are uninformed of the attacking scheme. Achievable single-letter expressions for the two kinds of error exponents are obtained. Single-letter lower bounds are also derived for the subclass of constant composition codes. These lower and the upper bounds coincide for the error exponent of the first class. Further, for the error of the first kind, a decoder that is optimal is introduced, and the worst case attack channel is characterized [J457]

"Analysis and Design of Finite-Length LDPC Codes"

We consider the performance analysis and code construction of finite-length low-density parity-check (LDPC) codes. First, by convergence analysis based on the extrinsic information evolution, we analyze the performance of both regular and irregular finite-length LDPC codes under iterative decoding. Next, by focusing on a special class of LDPC codes, namely, systematic irregular repeat-accumulate (IRA) codes, we propose a design procedure to construct finite-length LDPC codes. In addition to giving rise to a simple encoding structure, the special structure of IRA codes can be exploited to introduce unequal protection with cycle control for different types of nodes in the factor-graph code representation. We propose a modified bit-filling algorithm that leads to the construction of a set of finite-length IRA codes with low error floors [J458]

"Web dual watermarking technology using an XML document"

A novel dual watermark technology based on digital copyright technology is proposed, which, making full use of the advances of the web, stores the correlation information including the keys and the dual watermarks in an XML document. A new image watermarking technology to spread a digital image with copyright protection is realised successfully on the Internet. The arithmetic has very good robustness against the most common, non-malevolent data manipulations, including digital-to-analogue conversion and digital format conversion. Finally, the experimental results confirm that the two watermarks embedded by the proposed algorithm are invisible and robust against commonly used image-processing manipulations such as JPEG compression, adding noise, cropping, and rescaling and soon. The proposed algorithm is shown to provide very good results in term of image imperceptibility too [J459]

"A Survey and Analysis of the P3P Protocol's Agents, Adoption, Maintenance, and Future"

In this paper, we survey the adoption of the platform for privacy preferences protocol (P3P) on Internet Web sites to determine if P3P is a growing or stagnant technology. We conducted a pilot survey in February 2005 and our full survey in November 2005. We compare the results from these two surveys and the previous (July 2003) survey of P3P adoption. In general, we find that P3P adoption is stagnant, and errors in P3P documents are a regular occurrence. In addition, very little maintenance of P3P policies is apparent. These observations call into question P3P's viability as an online privacy-enhancing technology. Our survey exceeds other previous surveys in our use of both detailed statistical analysis and scope; our February pilot survey analyzed more than 23,000 unique Web sites, and our full survey in November 2005 analyzed more than 100,000 unique Web sites. [J460]

"Training and qualifying your employees"

Procedures alone cannot provide an improvement in electrical safety performance. Personnel who are exposed to electrical hazards must understand the basics of electrical hazards and safe work practices in order to implement the procedures. Training and qualifying your employees on these issues can be difficult and confusing. This article outlines a process for training employees on electrical safety issues. It will define "qualified" in terms that will satisfy the requirements of the Occupational Safety and Health Administration (OSHA) and NFPA 70E of the National Fire Protection Agency (NFPA) and also define the steps to meet the requirements of being qualified. The information contained in this article is the result of training the author has performed with electricians and nonelectrical personnel. The information is based upon the interpretation of the author. Employers should review the information and compare it to their interpretation of the regulations. [J461]

"Fast Worm Containment Using Feedback Control"

In a computer network, network security is accomplished using elements such as firewalls, hosts, servers, routers, intrusion detection systems, and honey pots. These network elements need to know the nature or anomaly of the worm a priori to detect the attack. Modern viruses such as Code Red, Sapphire, and Nimda spread quickly. Therefore, it is impractical if not impossible for human mediated responses to these fast-spreading viruses. Several epidemic studies show that automatic tracking of resource usage and control provides an effective method to contain the damage. In this paper, we propose a novel security architecture based on the control system theory. In particular, we describe a state-space feedback control model that detects and control the spread of these viruses or worms by measuring the velocity of the number of new connections an infected host makes. The mechanism's objective is to slow down a worm's spreading velocity by controlling (delaying) the number of new connections made by an infected host. A proportional and integral (PI) controller is used for a continuous control of the feedback loop. The approach proposed here has been verified in a laboratory setup, and we were able to contain the infection so that it affected less than 5 percent of the hosts. We have also implemented a protocol for exchanging control-specific information between the network elements. The results from the simulation and experimental setup combined with the sensitivity analysis demonstrate the applicability and accuracy of the approach. [J462]

"Virtual perimeter security (VPS) in a physical protection system"

There is a need to provide response force personnel with advanced warning of intruder activity in rough terrain outside the traditional facility perimeter. Often the land surrounding a high consequence facility is remote and difficult to sensor with conventional long-range detection systems. In order to combat this difficult problem, Sandia has investigated, developed, and fielded a wireless sensor network that demonstrated the value of providing advanced information of adversary activities. The project used wireless technologies to detect and assess intruders in remote "un-engineered" terrain around a fixed facility. In the time since the wireless intrusion detection system was fielded, minimal time has been spent on maintenance and no batteries required replacement. Sandia's wireless sensor network provides advanced warning of intruder activities and its installation will improve the security posture of a facility [J463]

"Scholarship for Service: New Mexico Tech's Undergraduate Program"

The scholarship for service program educates and prepares students for leadership roles in government positions in information assurance. SFS gives me the opportunity to support some of the best students at the New Mexico Institute of Mining and Technology and to work closely with them in their education, professional development, and research. In this article, the author focuses on the education of NMT's undergraduate SFS students [J464]

"Privacy-Preserving Data Mining Systems"

Although successful in many applications, data mining poses special concerns for private data. An integrated architecture takes a systemic view of the problem, implementing established protocols for data collection, inference control, and information sharing. Our goal in investigating privacy preservation issues was to take a systemic view of architectural requirements and design principles and explore possible solutions that would lead to guidelines for building practical privacy-preserving data mining systems [J465]

"A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks"

Attack mitigation schemes actively throttle attack traffic generated in distributed denial-of-service (DDoS) attacks. This paper presents attack diagnosis (AD), a novel attack mitigation scheme that adopts a divide-and-conquer strategy. AD combines the concepts of pushback and packet marking, and its architecture is in line with the ideal DDoS attack countermeasure paradigm-attack detection is performed near the victim host and packet filtering is executed close to the attack sources. AD is a reactive defense mechanism that is activated by a victim host after an attack is detected. By instructing its upstream routers to mark packets deterministically, the victim can trace back one attack source and command an AD-enabled router close to the source to filter the attack packets. This process isolates one attacker and throttles it, which is repeated until the attack is mitigated. We also propose an extension to AD called parallel attack diagnosis (PAD) that is capable of throttling traffic coming from a large number of attackers simultaneously. AD and PAD are analyzed and evaluated using the Skitter Internet map, Lumeta's Internet map, and the 6-degree complete tree topology model. Both schemes are shown to be robust against IP spoofing and to incur low false positive ratios [J466]

"Aiding Side-Channel Attacks on Cryptographic Software With Satisfiability-Based Analysis"

Cryptographic algorithms, irrespective of their theoretical strength, can be broken through weaknesses in their implementations. The most successful of these attacks are side-channel attacks which exploit unintended information leakage, e.g., timing information, power consumption, etc., from the implementation to extract the secret key. We propose a novel framework for implementing side-channel attacks where the attack is modeled as a search problem which takes the leaked information as its input, and deduces the secret key by using a satisfiability solver, a powerful Boolean reasoning technique. This approach can substantially enhance the scope of side-channel attacks by allowing a potentially wide range of internal variables to be exploited (not just those that are trivially related to the key). The proposed technique is particularly suited for attacking cryptographic software implementations which may inadvertently expose the values of intermediate variables in their computations (even though, they are very careful in protecting secret keys through the use of on-chip key generation and storage). We demonstrate our attack on standard software implementations of three popular cryptographic algorithms: DES, 3DES, and AES. Our attack technique is automated and does not require mathematical expertise on the part of the attacker [J467]

"Robust Data Hiding in Audio Using Allpass Filters"

A novel technique is proposed for data hiding in digital audio that exploits the low sensitivity of the human auditory system to phase distortion. Inaudible but controlled phase changes are introduced in the host audio using a set of allpass filters (APFs) with distinct parameters of allpass filters, i.e., pole-zero locations. The APF parameters are chosen to encode the embedding information. During the detection phase, the power spectrum of the audio data is estimated in the z-plane away from the unit circle. The power spectrum is used to estimate APF pole locations, for information decoding. Experimental results show that the proposed data hiding scheme can effectively withstand standard data manipulation attacks. Moreover, the proposed scheme is shown to embed 5-8 times more data than the existing audio data hiding schemes while providing comparable perceptual performance and robustness [J468]

"Near-Optimal Watermark Estimation and Its Countermeasure: Antidisclosure Watermark for Multiple Watermark Embedding"

Robustness is a critical requirement for a watermarking scheme to be practical. Current watermarking methods

usually claim a certain degree of robustness against those attacks that aim to destroy a hidden watermark at the expense of degrading the quality of the media data. However, there exist watermark-estimation attack (WEA), such as the collusion attack, which can remove watermarks while making the attacked data further transparent to its original. Another kind of attack is the copy attack, which can cause protocol ambiguity within a watermarking system. The aim of this paper is to deal with the WEA, which is clever at disclosing hidden information for unauthorized purposes. To this end, we begin by gaining insight into the WEA, leading to formal definitions of optimal watermark estimation and near-perfect cover data recovery. Subject to these definitions, a new content-dependent watermark (CDW) is proposed to deal with watermark-estimation attack. Mathematical analyses and experimental results consistently verify the effectiveness of the proposed watermark estimation and recovery algorithm, and the proposed content-dependent watermark. To our knowledge, this anti-disclosure watermark is the first work that can give those multiple-redundant watermark embedding approaches resistance to both collusion and copy attacks [J469]

"A New Approach Traveling-Wave Distance Protection—Part I: Algorithm"

This paper describe a new ultra-high speed protection algorithm for traveling-wave distance protection for transmission lines, based on pattern recognition of the first wavefront that arrives at the relay location due to fault. The algorithm uses principal component analysis (PCA) to preprocess data from the power system in order to eliminate redundant information and enhance hidden patterns in the traveling waves for internal and external faults. The algorithm was proven using PSCAD/EMTDC simulations in a three-phase 400-kV power system considering critical fault cases. The results show the feasibility to implement this algorithm for transmission-line ultra-high speed protection [J470]

"A Data Integration Broker for Healthcare Systems"

A prototype information broker uses a software service model to collect and integrate diverse patient data from autonomous healthcare agencies, potentially solving many problems that challenge current enterprise-based file systems [J471]

"The Technical Writer's Role in Preserving Intellectual Property Rights Outside the United States Tutorial"

This tutorial introduces issues regarding dissemination of information and texts that can affect international intellectual property rights. Four areas of concern for technical communicators include: (1) US and international rules about the disclosure of ideas and inventions; (2) corporate policies about confidentiality; (3) the complexities of international enforcement of intellectual property; and (4) principles of keeping records, including laboratory notebooks, that show ownership (including ownership of business methods). The training approach stresses a multipart program that includes understanding the patenting process; understanding and supporting corporate policies; and participating in dialogue about situations involving dissemination of information. This training should prepare technical communicators to evaluate or to recognize when to seek help from counsel in evaluating whether information should be disseminated. [J472]

"A Scalable Path Protection Mechanism for Guaranteed Network Reliability Under Multiple Failures"

We propose two versions of Link Failure Probability (LFP) based backup resource sharing algorithms, namely LFP based First-Fit algorithm, and LFP based Best-Fit algorithm for Generalized Multi-Protocol Label Switching networks. Customers' availability requirements are met by adjusting the availability of the protection paths with different sharing options. Information required for calculating the availability of both the working, and protection paths can be collected along the specific working, and protection paths, thus avoiding the requirement for flooding. This makes our algorithms scalable for a large network. Our algorithms work consistently against both single, and multiple failures. Furthermore, we propose extensions for the existing signaling protocols to demonstrate that our proposed algorithms require minimum changes to the existing protocols. Simulation results show that our proposal performs better than the conventional Dedicated Path Protection schemes in terms of Call Acceptance Rate, and Total Bandwidth Consumption. Finally, by comparing simulation results to analytical results for a simplified network, we provide some insights into the correctness, and efficiency of our proposed algorithms [J473]

"Discryption: Internal Hard-Disk Encryption for Secure Storage"

There have been many recent cases of information getting into unauthorized hands from lost or stolen laptops or insiders accessing unattended enterprise computers or storage devices. Providing physical protection and using

remote locations are two means of keeping stored data confidential. The least expensive secure-storage systems use local data encryption with optional data authentication, together with access control and physical tamper detection. The IEEE P1619 Security in Storage Working Group is developing standard architectures for external encryption modules and tape drives. However, there's no standard yet for hard disks, specifying how developers can adapt the data layout to security needs and provide access control to the encrypted data. That means an attacker can only see the ciphertext after disassembling the drive and examining the magnetic platters with multimillion-dollar equipment. And because of the attacks' destructive nature, if the disk drive is returned, the owner will notice the disk was tampered with and won't trust the stored information. This effectively renders all kinds of data-modification attacks harmless. [J474]

"Educating Students to Create Trustworthy Systems"

Computer science's long-standing tradition of computer security education has focused primarily on designing secure and reliable systems that can ensure information confidentiality, integrity, and availability. This tradition is geared toward preparing students for typical paradigms, such as writing secure code, providing authentication and access control, and developing policies to limit exposure to vulnerabilities and protect users' rights. Faculty and industry must find novel, cross-disciplinary approaches to educating security professionals to fully address this array of issues. In this article, we analyze barriers to effective security education and offer suggestions for improving cooperation among computer science, business management, information systems. and other technology departments. [J475]

"Building Privacy into Software Products and Services"

In the marketplace, customer trust is paramount. As consumers increasingly rely on the Internet for shopping, banking, and other daily activities, privacy is both a major public concern and a barrier to e-commerce growth: fear of data breaches and identity theft threaten to erode trust in the Internet. Once the core privacy team (CPT) is built, it can begin to define the program, deploy its processes, and enforce the rules. [J476]

"Software Protection through Anti-Debugging"

This article focuses on describing state-of-the-art attacks on debuggers to prevent reverse engineering. You can use the information we present as part of your strategy to protect your software or to assist you in overcoming the anti-debugging tricks present in malicious software. Currently, there are enough anti-debugging techniques available to software engineers to sufficiently protect software against most threats, likewise, most state-of-the-art malware can be sufficiently reverse-engineered with patience and skill to enable security researchers to continue to defend their networks. However, advances in software protection techniques and reverse engineering might alter the balance. [J477]

"Supporting Resource-Constrained Collaboration Environments"

The many collaboration and document-management products available today help establish controls over document workflows. Essentially, these applications automate information categorization, filing, version control, and historical tracking. The advent of products that help find the necessary but long-forgotten documents needed to complete a task has spurred demand for these applications. Organizations with document collaboration requirements clearly benefit from this technology. Computing professionals, in turn, play an important role in identifying the most appropriate technology for the collaboration problem at hand. Unfortunately, resources are not always available to acquire the needed product. Document-management and collaboration tools can be cost-prohibitive to many organizations. This does not bode well for resource-constrained organizations that need some form of information management. However, computing professionals can propose nonautomated solutions to accommodate manual problems, such as file-naming conventions and document versioning, through the appropriate use of the technology at hand. Although automated tools are more attractive and exciting, making such acquisitions is not always feasible. [J478]

"Context Information-Based Cyber Security Defense of Protection System"

With the development of a substation automation system, it is now feasible for the intelligent electronic devices-based protection system to collect its measurements from electronic instrument transformers through a communication network such as an Ethernet-based local-area network. The application of a wide-area broadband network in power utilities introduces underlying danger for protection systems to maloperate when receiving fake data packages from an intruder. This paper proposes identifying a vicious fault by using context information, such as voltage and current, of the same substation. When the protection system detects a fault based on measurements transmitted through a network, it collects all measurements of the substation and feeds these data to a probabilistic neural network. Thereafter, the fault caused by fake data that differs from the known

fault pattern can be identified and blocked. [J479]

"An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price"

Security defects in software cost millions of dollars to firms in terms of downtime, disruptions, and confidentiality breaches. However, the economic implications of these defects for software vendors are not well understood. Lack of legal liability and the presence of switching costs and network externalities may protect software vendors from incurring significant costs in the event of a vulnerability announcement, unlike such industries as auto and pharmaceuticals, which have been known to suffer significant loss in market value in the event of a defect announcement. Although research in software economics has studied firms' incentives to improve overall quality, there have not been any studies which show that software vendors have an incentive to invest in building more secure software. The objectives of this paper are twofold. 1) We examine how a software vendor's market value changes when a vulnerability is announced. 2) We examine how firm and vulnerability characteristics mediate the change in the market value of a vendor. We collect data from leading national newspapers and industry sources, such as the Computer Emergency Response Team (CERT), by searching for reports on published software vulnerabilities. We show that vulnerability announcements lead to a negative and significant change in a software vendor's market value. In our sample, on average, a vendor loses around 0.6 percent value in stock price when a vulnerability is reported. We find that a software vendor loses more market share if the market is competitive or if the vendor is small. To provide further insight, we use the information content of the disclosure announcement to classify vulnerabilities into various types. We find that the change in stock price is more negative if the vendor fails to provide a patch at the time of disclosure. Also, more severe flaws have a significantly greater impact. Our analysis provides many interesting implications for software vendors as well as policy make- rs. [J480]

"Modeling Drug Mechanism Knowledge Using Evidence and Truth Maintenance"

To protect the safety of patients, it is vital that researchers find methods for representing drug mechanism knowledge that support making clinically relevant drug-drug interaction (DDI) predictions. Our research aims to identify the challenges of representing and reasoning with drug mechanism knowledge and to evaluate potential informatics solutions to these challenges through the process of developing a knowledge-based system capable of predicting clinically relevant DDIs that occur via metabolic mechanisms. In previous work, we designed a simple, rule-based, model of metabolic inhibition and induction and applied it to a database containing assertions about 267 drugs. This pilot system taught us that drug mechanism knowledge is often dynamic, missing, or uncertain. In this paper, we propose methods to address these properties of mechanism knowledge and describe a new prototype system, the Drug Interaction Knowledge-base (DIKB), that implements our proposed methods so that we can explore their strengths and limitations. A novel feature of the DIKB is its use of a truth maintenance system to link changes in the evidence support for assertions about drug properties to the set of interactions and non-interactions the system predicts. [J481]

"Self-Orthogonality of q -Ary Images of qm -Ary Codes and Quantum Code Construction"

A code over GF can be imaged or expanded into a code over GF using a basis for the extension field over the base field. The properties of such an image depend on the original code and the basis chosen for imaging. Problems relating the properties of a code and its image with respect to a basis have been of great interest in the field of coding theory. In this work, a generalized version of the problem of self-orthogonality of the q-ary image of a qm-ary code has been considered. Given an inner product (more generally, a bi-additive form), necessary and sufficient conditions have been derived for a code over a field extension and an expansion basis so that an image of that code is self-orthogonal. The conditions require that the original code be self-orthogonal with respect to several related bi-additive forms whenever certain power sums of the dual basis elements do not vanish. Numerous interesting corollaries have been derived by specializing the general conditions. An interesting result for the canonical or regular inner product in fields of characteristic two is that only self-orthogonal codes result in self-orthogonal images. Another result is that image of a code is self-orthogonal for all bases if and only if trace of the code is self-orthogonal, except for the case of binary images of 4-ary codes. The conditions are particularly simple to state and apply for cyclic codes. To illustrate a possible application, new quantum error-correcting codes have been constructed with larger minimum distance than previously known. [J482]

"Building Knowledge for Substation-Based Decision Support Using Rough Sets"

This paper describes a new technique based on rough sets to extract decision rules from large volumes of data captured by protection, control, and monitoring intelligent electronic devices. The methodology correctly identifies faults from large datasets and could be used to assist operators in their decision-making processes. Building knowledge for a fault diagnostic system is a time-consuming and costly process. The quality of a knowledge

base can sometimes be hampered by a large number of superfluous decision-making rules that can lead to an unnecessarily large knowledge base system and inefficient or even detrimental rule maintenance. The methodology proposed cannot only induce decision rules efficiently but can also reduce the size of the knowledge base without causing loss of useful information. Results can be used by an expert system to generate supervisory automation and to support operators, for example, during an emergency situation. This methodology involves the generation of human-machine interface alarms. These can then be used for diagnosis of the type and cause of a fault event to give suggestions for network restoration and post-emergency repair. A power systems computer aided design/electromagnetic transients including dc simulator has been used to investigate the effect of faults and switching actions on the protection and control equipment associated with a typical distribution network. The fundamental ideas of rough set theory are discussed, followed by a rule assessment method that is outlined using an illustrative example. [J483]

"Stochastic Estimation of Voltage Sags in a Large Meshed Network"

This paper presents a method for stochastic prediction of voltage sags caused by faults in a power system. The area of vulnerability must be determined to estimate the expected sag frequency (ESF) at a sensitive load site. However, the area of vulnerability is not easy to identify in a large meshed network. In the paper, the residual phase voltage equations for balanced and unbalanced faults are presented, and an efficient method to determine the area of vulnerability in a large meshed network is described. An ESF estimation method based on information technology industry council (ITIC) curve is also described. The developed method was applied to the IEEE 30-bus test system. [J484]

"A Coherent Strategy for Data Security through Data Governance"

The role of boards of directors now extends to ensuring that a company's data is actively managed in an increasingly technology-intense environment. In this article, the authors show how this requires greater attention to legislative requirements, greater due diligence in transactions and business alliances, and coherent information management strategies. [J485]

"Optical Watermarking for Printed Document Authentication"

This article describes a novel visual information concealment technique, referred to as optical watermarking, for the authentication of original printed documents. An optical watermark is a two-dimensional binary image. It can be of any shape and can be printed on any part of a document. The optical watermark is constructed by the superposition of multiple two-dimensional binary images (referred to as layers), each with different carrier structural patterns embedding various hidden information. The hidden information is embedded into each layer using phase modulation. Based on properties of the human visual system and modulation principle, the hidden information becomes visible to the human eyes only when a right "key" is positioned on top of the optical watermark with the right alignment. Here, "keys" play the similar role as keys in encryption, that is, to decode hidden information. Thus, with such a "lock and key" approach, it greatly improves the security level of the optical watermark. In addition, the multiple layer structure of the optical watermark makes it extremely robust against reverse engineering attacks. Due to its high security and tight link with electronic document systems, which requires documents to be finally printed on paper, the optical watermark has been applied to various electronic document systems. These are online ticketing, online bill of lading, and remote signing and printing of documents, where critical and unique information are embedded in watermarks and printed together with individual documents for future authentication. It has also been used in offline and traditional antiforgery applications, such as brand protection, preprinted high-value tickets, and identification documents [J486]

"Analysis and Protection of Dynamic Membership Information for Group Key Distribution Schemes"

In secure group-oriented applications, key management schemes are employed to distribute and update keys such that unauthorized parties cannot access group communications. Key management, however, can disclose information about the dynamics of group membership, such as the group size and the number of joining and departing users. This is a threat to applications with confidential group membership information. This paper investigates techniques that can stealthily acquire group dynamic information from key management. We show that insiders and outsiders can successfully obtain group membership information by exploiting key establishment and key updating procedures in many popular key management schemes. Particularly, we develop three attack methods targeting tree-based centralized key management schemes. Further, we propose a defense technique utilizing batch rekeying and phantom users, and derive performance criteria that describe security level of the proposed scheme using mutual information. The proposed defense scheme is evaluated based on the data from MBone multicast sessions. We also provide a brief analysis on the disclosure of group dynamic information in contributory key management schemes [J487]

"Securing Cooperative Ad-Hoc Networks Under Noise and Imperfect Monitoring: Strategies and Game Theoretic Analysis"

In cooperative ad-hoc networks, nodes belong to the same authority and pursue the common goals, and will usually unconditionally help each other. Consequently, without necessary countermeasures, such networks are extremely vulnerable to insider attacks, especially under noise and imperfect monitoring. In this paper, we present a game theoretic analysis of securing cooperative ad-hoc networks against insider attacks in the presence of noise and imperfect monitoring. By focusing on the most basic networking function, namely routing and packet forwarding, we model the interactions between good nodes and insider attackers as secure routing and packet forwarding games. The worst case scenarios are studied where initially good nodes do not know who the attackers are while insider attackers know who are good. The optimal defense strategies have been devised in the sense that no other strategies can further increase the good nodes' payoff under attacks. Meanwhile, the optimal attacking strategies and the maximum possible damage that can be caused by attackers have been discussed. Extensive simulation studies have also been conducted to evaluate the effectiveness of the proposed strategies [J488]

"Simulated annealing-based optimal wind-thermal coordination scheduling"

The rise of environmental protection and the progressive exhaustion of traditional fossil energy sources have increased the interests in integrating wind energy sources into existing power systems. Development of better wind-thermal coordination algorithms is necessary to determine the optimal proportion of wind generator capacity that can be integrated into the system for operating an isolated hybrid power system reliably and efficiently. A stochastic searching technique, which utilises a simulated annealing (SA) approach combined with an efficient constrained dynamic economic dispatch (CDED) method, is developed to coordinate the wind and thermal generation scheduling in isolated power systems with large integration of wind capacity. The SA algorithm is used for the scheduling of the generating units, whereas a direct search method routine carries out the ramp rate CDED when considering wind power generation. Several technique constraints are applied to determine the maximum proportion of wind generator capacity that can be integrated into the system. A constraint satisfaction technique for generating feasible neighbouring solution is also developed to improve the SA solution process. Numerical experiments are included to understand the wind generator capacity in the operating cost analysis and to provide valuable information for both the operational and planning problems [J489]

"Strong Diffie-Hellman-DSA Key Exchange"

To provide authentication to the Diffie-Hellman key exchange, a few integrated key exchange schemes which provide authentication using the DSA signature have been proposed in the literature. In this letter we point out that all of the previous Diffie-Hellman-DSA schemes do not provide security against session state reveal attacks. We also suggest a strong Diffie-Hellman-DSA scheme providing security against session state reveal attacks as well as forward secrecy and key independence [J490]

"A Constructive and Unifying Framework for Zero-Bit Watermarking"

In the watermark detection scenario, also known as zero-bit watermarking, a watermark, carrying no hidden message, is inserted in a piece of content. The watermark detector checks for the presence of this particular weak signal in received contents. The article looks at this problem from a classical detection theory point of view, but with side information enabled at the embedding side. This means that the watermark signal is a function of the host content. Our study is twofold. The first step is to design the best embedding function for a given detection function, and the best detection function for a given embedding function. This yields two conditions, which are mixed into one 'fundamental' partial differential equation. It appears that many famous watermarking schemes are indeed solution to this 'fundamental' equation. This study thus gives birth to a constructive framework unifying solutions, so far perceived as very different [J491]

"Noncollaborative Resource Management for Wireless Multimedia Applications Using Mechanism Design"

We propose to add a new dimension to existing wireless multimedia communications systems by enabling competing stations to proactively engage in the resource management game by adapting their cross-layer transmission strategies. For this, we model wireless stations (WSTAs) as rational and selfish players competing for available wireless resources in a dynamic game. We focus on polling-based wireless LAN (WLAN) networks, where developing an efficient solution for managing the available transmission opportunities is of paramount importance. The resource allocation game is coordinated by a network moderator, which deploys a novel resource management based on the Vickrey-Clarke-Groves (VCG) mechanism to determine a) the amount of

time to be allocated to the various users and b) the transmission cost associated to the allocated resources. The transmission cost is referred to in the VCG mechanism as "transfer" and depends not on the used resources, but rather on the inconvenience (in terms of utility impact) that it causes to other WSTAs. The transfer is introduced in order to discourage WSTAs from lying about their resource requirements. Importantly, this proposed dynamic resource management approach for wireless multimedia applications changes the passive way stations are currently adapting their cross-layer strategies by enabling them to selfishly influence the wireless systems dynamics by proactively adapting their packet scheduling strategies, error protection strategies, etc. Hence, each wireless station can play the resource management game by adapting its multimedia transmission strategy depending on the experienced channel conditions, derived video quality, attitude towards risk, willingness to pay for resources and available information about the wireless network. Our simulations show that using the VCG mechanism the WSTAs do not have any incentives to lie about their resource requirements as otherwise they will be severely penalized by a high transfer. We also-- show that deploying advanced cross-layer strategies for playing the resource management game significantly benefit the WSTAs' received video quality. The willingness-to-pay for resources is introduced to provide WSTAs a tool to gather additional resources whenever they need to transmit an important (part of a) video sequence by agreeing to pay for resources an increased cost. A novel risk-aware scheduling scheme is also proposed that provides WSTAs the ability to dynamically avoid network congestion and hence, reduce their incurred transfer [J492]

"Guest Editors' Introduction: Managing Organizational Security"

In this special issue, we focus on the challenges of managing organizational security, examining some of the nontechnical aspects of security that assure that the technology is chosen, implemented, and used appropriately and well. [J493]

"Embedding Information Security into the Organization"

Risk and business have always been inseparable, but new information security risks pose unknown challenges. How should firms organize and manage to improve enterprise security? Here, the authors describe how chief information security officer (CISOs) are working to build secure organizations. [J494]

"I'll Buy That! Cybersecurity in the Internet Marketplace"

Interviews with chief security officers in the Internet supply chain (those companies that provide Internet services or encourage people to use the Internet) reveal dramatically different attitudes about corporate cybersecurity. The authors' preliminary investigation suggests that a company's market discipline explains these differences. [J495]

"Distributed Joint Source-Channel Coding of Video Using Raptor Codes"

Extending recent works on distributed source coding, this paper considers distributed source-channel coding and targets at the important application of scalable video transmission over wireless networks. The idea is to use a single channel code for both video compression (via Slepian-Wolf coding) and packet loss protection. First, we provide a theoretical code design framework for distributed joint source-channel coding over erasure channels and then apply it to the targeted video application. The resulting video coder is based on a cross-layer design where video compression and protection are performed jointly. We choose Raptor codes-the best approximation to a digital fountain-and address in detail both encoder and decoder designs. Using the received packets together with a correlated video available at the decoder as side information, we devise a new iterative soft-decision decoder for joint Raptor decoding. Simulation results show that, compared to one separate design using Slepian-Wolf compression plus erasure protection and another based on FGS coding plus erasure protection, the proposed joint design provides better video quality at the same number of transmitted packets. Our work represents the first in capitalizing the latest in distributed source coding and near-capacity channel coding for robust video transmission over erasure channels. [J496]

"Spare Capacity Allocation in Two-Layer Networks"

In this paper we consider the problem of provisioning spare capacity in two-layer backbone networks using shared backup path protection. First, two spare capacity allocation (SCA) optimization problems are formulated as integer linear programming (ILP) models for the cases of protection at the top layer against failures at the bottom layer. The first model captures failure propagation using overlay information between two layers for backup paths to meet diversity requirements. The second model improves bandwidth efficiency by moving spare capacity sharing from the top layer to the bottom layer. This exposes a tradeoff between bandwidth efficiency and extra cross-layer operation. Next, the SCA model for common pool protection is developed to allow spare capacity sharing between two layers. Our previous SCA heuristic technique, successive survivable routing (SSR)

is extended for these optimization problems. Numerical results for a variety of networks indicate that the common pool protection is attractive to enhance bandwidth efficiency without loss of survivability and that the SSR heuristic quickly results in near optimal solutions [J497]

"Toward effective substation automation"

Integrating IEC61850 at TVA's Bradley substation for protection, SCADA, and enterprise applications substation, and enterprise applications. The IEC 61850 standard provides the means to integrate communications, information, and applications into a coherent, flexible, very powerful framework for the secondary system. With its deployment, more information can be exchanged and more applications can be run. And we shall see that integrated, accessible information is truly the enabler of effective and economic substation automation [J498]

"Transmission Line Boundary Protection Using Wavelet Transform and Neural Network"

Two of the most expected objectives of transmission line protection are: 1) differentiating precisely the internal faults from external and 2) indicating exactly the fault type using one end data only. This paper proposes an improved solution based on wavelet transform and self-organized neural network. The measured voltage and current signals are preprocessed first and then decomposed using wavelet multiresolution analysis to obtain the high frequency details and low frequency approximations. The patterns formed based on high frequency signal components are arranged as inputs of neural network #1, whose task is to indicate whether the fault is internal or external. The patterns formed using low frequency approximations are arranged as inputs of neural network #2, whose task is to indicate the exact fault type. The new method uses both low and high frequency information of the fault signal to achieve an advanced line protection scheme. The proposed approach is verified using frequency-dependent transmission line model and the test results prove its enhanced performance. A discussion of the application issues for the proposed approach is provided at the end where the generality of the proposed approach and guidance for future study are pointed out [J499]

"New Challenges for the New Year"

You've heard from me in this space before, but this is my first column as IEEE Security & Privacy's editor in chief. I feel both honored and privileged to have the opportunity to assume this responsibility. George Cybenko, as both the driving force behind the magazine's creation and its EIC for the first four years, is a hard act to follow. But because he created such a strong base for the magazine, I'm hoping it won't be a difficult act to continue. You can expect the mix of articles, departments, and special issues on current topics to continue. You'll see some new names in the masthead as we replace those rotating off the editorial board; this is a normal process for all IEEE publications. We'll continue to strive for fresh and interesting material to keep you at the forefront of technology and issues in security and privacy. [J500]

"Is Information Security Under Control?: Investigating Quality in Information Security Management"

Over the past decade, organizations have sought to become more efficient and productive by adopting information and communication technologies. Organizations are consequently more aware of information security risks and the need to take appropriate action. Previous studies of organizations' use of information security controls have focused on the presence or absence of controls, rather than their quality. We designed and conducted a survey as an initial step toward meeting this challenge. To do this, we benchmarked how organizations manage information security by implementating various controls. Although security surveys are nothing new, our method aims to uncover specific details of control implementation and focus on implementation quality. With a more precise understanding of current practices, information security management can begin to properly pursue effective strategies to improve quality and lower risk [J501]

"Slaying the Academia Beast [JThe Ivory Tower]"

Sorel Reisman discusses the world view of academia and how "members of the academy" need a dose of reality before they bash the for-profit world. [J502]

"An Information Avalanche"

The Internet has added yet another dimension to the production and consumption of information. Long merely consumers of content, Internauts are now also major producers of it. Search engines make it possible to sift through the enormous quantity of material that is finding its way into digital form. Going online has become an adventure in discovery for those who eagerly surf the billions of Web pages housed in the global Internet. Because of its global reach, the Internet seriously threatens to undermine IP protection regimes that have long served copyright holders [J503]

"Using Environmental Models to Optimize Sensor Placement"

Sensors used in protective applications are conventionally placed on perimeters or over areas in an evenly distributed pattern. However, such patterns may actually be suboptimal, since environmental factors may make some forms of attack more or less likely than others. We describe a protective application of sensors for detecting underwater threats in an urban estuary environment. We demonstrate that environmental information, derived from a computational river current model, can be utilized to optimize sensor placement, increasing detection rates and decreasing the number of required sensors. Simulation results show a significant improvement in detection likelihood for a given number of sensors; alternatively, fewer sensors can be used while still maintaining the detection rate of a conventional approach [J504]

"Nonintrusive Component Forensics of Visual Sensors Using Output Images"

Rapid technology development and the widespread use of visual sensors have led to a number of new problems related to protecting intellectual property rights, handling patent infringements, authenticating acquisition sources, and identifying content manipulations. This paper introduces nonintrusive component forensics as a new methodology for the forensic analysis of visual sensing information, aiming to identify the algorithms and parameters employed inside various processing modules of a digital device by only using the device output data without breaking the device apart. We propose techniques to estimate the algorithms and parameters employed by important camera components, such as color filter array and color interpolation modules. The estimated interpolation coefficients provide useful features to construct an efficient camera identifier to determine the brand and model from which an image was captured. The results obtained from such component analysis are also useful to examine the similarities between the technologies employed by different camera models to identify potential infringement/licensing and to facilitate studies on technology evolution [J505]

"Security Analysis of Multimedia Encryption Schemes Based on Multiple Huffman Table"

This letter addresses the security issues of the multimedia encryption schemes using multiple Huffman table (MHT). A known-plaintext attack is presented to show that the MHTs used for encryption should be carefully selected to avoid the weak keys problem. We then propose chosen-plaintext attacks on the basic MHT algorithm as well as the enhanced scheme with random bit insertion. In addition, we suggest two empirical criteria for Huffman table selection, based on which we can simplify the stream cipher integrated scheme, while ensuring a high level of security [J506]

"A Framework for Robust Watermarking of H.264-Encoded Video With Controllable Detection Performance"

As H.264 digital video becomes more prevalent, the need for copyright protection and authentication methods that are appropriate for this standard will emerge. This paper proposes a robust watermarking algorithm for H.264. We employ a human visual model adapted for a 4 times 4 discrete cosine transform block to increase the payload and robustness while limiting visual distortion. A key-dependent algorithm is used to select a subset of the coefficients that have visual watermarking capacity. Furthermore, the watermark is spread over frequencies and within blocks to avoid error pooling. This increases the payload and robustness without noticeably changing the perceptual quality. We embed the watermark in the coded residuals to avoid decompressing the video; however, we detect the watermark from the decoded video sequence in order to make the algorithm robust to intraprediction mode changes. We build a theoretical framework for watermark detection based on a likelihood ratio test. This framework is used to obtain optimal video watermark detection with controllable detection performance. Our simulation results show that we achieve the desired detection performance in Monte Carlo trials. We demonstrate the robustness of our proposed algorithm to several different attacks [J507]

"HIPAA's Effect on Web Site Privacy Policies"

Healthcare institutions typically post their privacy practices online as privacy policy documents. We conducted a longitudinal study that examines the effects of HIPAA's enactment on a collection of privacy policy documents for a fixed set of organizations over a four-year period. We present our analysis of 24 healthcare privacy policy documents from nine healthcare Web sites, analyzed using goal mining, a content-analysis method that supports extraction of useful information about institutions' privacy practices from documents. We compare our results to our pre-HIPAA study of these same institutions' online privacy practices and evaluate their evolution in the presence of privacy laws [J508]

"A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change

Tracking Technique"

A new steganographic method for data hiding in Microsoft Word documents by a change tracking technique is proposed. The data embedding is disguised such that the stegodocument appears to be the product of a collaborative writing effort. Text segments in the document are degenerated, mimicking to be the work of an author with inferior writing skills, with the secret message embedded in the choices of degenerations. The degenerations are then revised with the changes being tracked, making it appear as if a cautious author is correcting the mistakes. The change tracking information contained in the stegodocument allows the original cover, the degenerated document, and, hence, the secret message to be recovered. The extra change tracking information added during message embedding is vital in a normal collaboration scenario, and so hinders ignorant removals by skeptics. Experiments demonstrate the feasibility of the proposed method [J509]

"Evolutionary Algorithms Refining a Heuristic: A Hybrid Method for Shared-Path Protections in WDM Networks Under SRLG Constraints"

An evolutionary algorithm (EA) can be used to tune the control parameters of a construction heuristic to an optimization problem and generate a nearly optimal solution. This approach is in the spirit of indirect encoding EAs. Its performance relies on both the heuristic and the EA. This paper proposes a three-phase parameterized construction heuristic for the shared-path protection problem in wavelength division multiplexing networks with shared-risk link group constraints and applies an EA for optimizing the control parameters of the proposed heuristics. The experimental results show that the proposed approach is effective on all the tested network instances. It was also demonstrated that an EA with guided mutation performs better than a conventional genetic algorithm for tuning the control parameters, which indicates that a combination of global statistical information extracted from the previous search and location information of the best solutions found so far could improve the performance of an algorithm [J510]

"Cross-Layer Packetization and Retransmission Strategies for Delay-Sensitive Wireless Multimedia Transmission"

Existing wireless networks provide dynamically varying resources with only limited support for the quality of service required by the bandwidth-intense, loss-tolerant and delay-sensitive multimedia applications. This variability of resources does not significantly impact delay insensitive data transmission (e.g., file transfers), but has considerable consequences for multimedia applications. Recently, the research focus has been to adapt existing algorithms and protocols at the lower layers of the protocol stack to better support multimedia transmission applications and conversely, to modify application layer solutions to cope with the varying wireless networks resources. In this paper, we show that significant improvements in wireless multimedia performance can be obtained by deploying a joint application-layer adaptive packetization and prioritized scheduling and MAC-layer retransmission strategy. We deploy a state-of-the-art wavelet coder for the compression of the video data that enables on-the-fly adaptation to changing channel conditions and inherent prioritization of the video bitstream. We pose the cross-layer problem as a distortion minimization given delay constraints and derive analytical solutions by modifying existing joint source-channel coding theory aimed at fulfilling rate, rather than delay, constraints. We also propose real-time algorithms that explicitly consider the available information about previously transmitted packets. The obtained results show significant improvements in terms of video quality as opposed to ad-hoc optimizations currently deployed, while the complexity associated with performing this optimization in real time, i.e., at transmission time, is limited [J511]

"Render Sequence Encoding for Document Protection"

We present in this paper a novel electronic document watermarking method, render sequence encoding (RSE), and then further develop a RSE authentication method for electronic documents. RSE watermarks an electronic document by modulating the display sequences of words or characters. It features large information-carrying capacity and robustness over document format transcoding. The RSE authentication method is based on the NP-complete exact traveling salesman problem, which provides a rigorous foundation for security. The RSE authentication method is secure in the sense it is extremely difficult to forge the authentication process. RSE authentication process is also easy to operate, especially in comparison to digital signatures which requires public key infrastructure for its operation [J512]

"Introduction"

The regulatory landscape that enterprises face today has been characterized by an unrelenting increase in the number of governmental regulations. Since 1981, more than 118,000 regulations have been introduced in the United States alone. These include the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the well-known Patriot Act of 2001, and the Sarbanes-Oxley Act of 2002. Similar regulations, such as the Japanese

Personal Information Protection Act of April 2005, have been enacted in other countries. Other regulations, such as Basel II for the banking industry, have been issued by international agreement. Regulations have significantly increased the costs and the risks of doing business. The trend of business process outsourcing and the dynamics of disaggregated value nets only compound the challenge of dealing with compliance requirements. The concomitant explosion of information in enterprises adds to the challenge of leveraging that information to improve business performance while developing effective controls to manage the integrity and security of the information. [J513]

"Best practices and tools for personal information compliance management"

Recent incidents involving the loss of personal information and identity theft have raised concerns worldwide over information privacy. In Japan, the Personal Information Protection Act went into effect in April 2005, requiring every enterprise to manage sensitive personal information on servers, workstations, and personal computers throughout the organization. This paper describes two tools we developed to assist in the management of personal information, aDesigner and the Personal Information Detection (PID) tool. The aDesigner tool scans an entire Web site to determine if each HTML page complies with the IBM privacy guidelines for external Web sites. PID is capable of automatically identifying "named entities," such as personal names, addresses, or telephone numbers in the textual parts of target files based on Japanese morphological analysis technology. This paper also summarizes the best practices used in IBM Japan for privacy management and presents statistical results concerning personal information gathered through deployment of these tools. [J514]

"Compliance with data protection laws using Hippocratic Database active enforcement and auditing"

Governments worldwide are enacting data protection laws that restrict the disclosure and processing of personal information. These laws impose administrative and financial burdens on companies that manage personal information and may hinder the legitimate and valuable sharing and analysis of this information. In this paper we describe an integrated set of technologies, known as the Hippocratic Database (HDB), which enables compliance with security and privacy regulations without impeding the legitimate flow of information. HDB's Control Center allows companies to specify fine-grained disclosure policies based on the role of the user, the purpose of the access, the intended recipient, and other disclosure conditions. Its Active Enforcement component transparently enforces these policies by transforming user queries in a middleware layer to ensure that the database returns only policy-compliant information. HDB's Compliance Auditing system efficiently tracks all database accesses and allows auditors to formulate precise audit queries to monitor compliance with privacy and security policies. In this paper, we outline the basic architecture of the HDB solution, discuss the advantages of our approach, and illustrate the features of each component with practical compliance scenarios from the financial services industry. [J515]

"Experimental Investigation of Lightning Transients Entering a Swedish Railway Facility"

Transients caused by lightning in railway facilities have not received much attention. In this paper, we describe the measurements of lightning transients entering a Swedish railway facility during the summer of 2003. The measurements of the transients were made in a technical house that provides an uninterrupted power supply for telecommunication systems and the signal systems. An analysis of the data has shown that transients in excess of 7 kV (peak to peak) can appear across the line-to-neutral supply system due to an indirect lightning strike. Some typical characteristics of the line-to-neutral transient voltages in terms of stroke locations and stroke amplitudes are presented. Further, from the experimental data, an empirical relation for predicting the line-to-neutral transient voltage in terms of stroke location and stroke current amplitude is obtained. Simple induced voltage calculations are presented to identify the levels of induced voltages appearing at the input of the technical house. The influence of ground conductivity on those induced voltages is also presented. The information presented in the paper is an important electromagnetic-compatibility issue associated with the lightning protection for railway systems [J516]

"Bosch wireless IP solution provides crime protection [JBriefing contracts]"

{no data available} [J517]

"Fault Current Contribution From Synchronous Machine and Inverter Based Distributed Generators"

There are advantages of installing distributed generation (DG) in distribution systems: for example, improving reliability, mitigating voltage sags, unloading subtransmission and transmission system, and sometimes utilizing renewables. All of these factors have resulted in an increase in the use of DGs. However, the increase of fault

currents in power systems is a consequence of the appearance of new generation sources. Some operating and planning limitations may be imposed by the resulting fault currents. This paper discusses a model of inverter based DGs which can be used to analyze the dynamic performance of power systems in the presence of DGs. In a style similar to protective relaying analysis, three-dimensional plots are used to depict the behavior of system reactance (X) and resistance (R) versus time. These plots depict operating parameters in relation to zones of protection, and this information is useful for the coordination of protection systems in the presence of DG [J518]

"Fiber-Grating-Based Vision System for Real-Time Tracking, Monitoring, and Obstacle Detection"

There is a real need to develop a sensory system that can monitor and track the behavioral status of a person in real time while protecting his/her privacy. In addition, it is important to have the ability to detect stationary and moving objects in real time to support dynamic navigation needs for mobile robots. This paper describes the development of intelligent fiber-grating (FG)-based 3-D vision sensory system that enables real-time object detection, monitoring, and tracking. This system uses the richness and the strength of the vision while reducing the data load and computational cost by encoding the working space using a limited number of spatially interrelated 2-D laser spots. The sensor system generates the laser spots by projecting a coherent laser beam on two perpendicularly overlaid layers of FGs. The presence of a target within the visible operational view of the sensor disturbs the part of the projected laser spots' pattern where the target appeared. By calculating the displacement of the disturbed spots within the CCD image plane, the sensor system can detect, in a short time, an object/human and provide relevant information in terms of range, approximate shape, and position. To facilitate faster detection and real-time tracking, the author has developed two strategies that decompose the working space into zones and virtual planes [J519]

"Differential Protection Based on Zero-Sequence Voltages for Generator Stator Ground Fault"

This paper introduces a new differential protection scheme based on zero-sequence voltages with 100% coverage for generator stator ground faults. Analysis shows that the Delta-fundamental zero-sequence voltages and the Delta-third-harmonic voltages at the generator neutral and the terminals will change simultaneously, and they present some similar characteristics. According to that, the new scheme that exploits the fault information of both the zero-sequence fundamental voltage and the third-harmonic voltage is described. As it combines the information of the zero-sequence fundamental voltage and the third-harmonic voltage, the scheme can detect the ground fault with high sensitivity in 100% coverage winding. Simulation and field test results show that the proposed scheme can obtain higher sensitivity than the traditional schemes [J520]

"Influence of current transformer saturation on line current differential protection algorithms"

The performance of line current differential protection algorithms during current transformer (CT) saturation is analysed. The study covers popularly used algorithms and presents their degree of immunity to CT saturation. The degree of error in phasor measurement due to CT saturation is estimated through simulation studies and this information is used to decide the CT dimensioning for the relay [J521]

"Power transformer protection using S-transform with complex window and pattern recognition approach"

A new approach for power transformer protection using S-transform with complex window to distinguish between inrush current and internal fault is presented. The S-transform with complex window is used to extract patterns of transient current samples during inrush and faults. S-transform is a very powerful tool for non-stationary signal analysis giving the information of transient currents both in time and in frequency domains. The spectral energy is calculated for inrush and internal faults and an energy index is found out to distinguish between inrush magnetising current and internal faults. The simulation results and the results obtained using real-time data from a transformer in the laboratory environment indicate the robustness of the proposed technique [J522]

"Anonymizing Classification Data for Privacy Preservation"

Classification is a fundamental problem in data analysis. Training a classifier requires accessing a large collection of data. Releasing person-specific data, such as customer data or patient records, may pose a threat to an individual's privacy. Even after removing explicit identifying information such as Name and SSN, it is still possible to link released records back to their identities by matching some combination of nonidentifying attributes such as {Sex, Zip, Birthdate}. A useful approach to combat such linking attacks, called k-anonymization, is anonymizing the linking attributes so that at least k released records match each value combination of the linking attributes. Previous work attempted to find an optimal k-anonymization that minimizes

some data distortion metric. We argue that minimizing the distortion to the training data is not relevant to the classification goal that requires extracting the structure of predication on the "future" data. In this paper, we propose a k-anonymization solution for classification. Our goal is to find a k-anonymization, not necessarily optimal in the sense of minimizing data distortion, which preserves the classification structure. We conducted intensive experiments to evaluate the impact of anonymization on the classification on future data. Experiments on real-life data show that the quality of classification can be preserved even for highly restrictive anonymity requirements [J523]

"On Z2k -Dual Binary Codes"

A new generalization of the Gray map is introduced. The new generalization Phi:Z2knrarr Z22k-1n is connected with the known generalized Gray map phi in the following way: if we take two dual linear Z2 k-codes and construct binary codes from them using the generalizations phi and Phi of the Gray map, then the weight enumerators of the binary codes obtained will satisfy the MacWilliams identity. The classes of Z2k-linear Hadamard codes and co-Z2k-linear extended 1-perfect codes are described, where co-Z2k-linearity means that the code can be obtained from a linear Z2k-code with the help of the new generalized Gray map [J524]

"Rateless Codes With Unequal Error Protection Property"

In this correspondence, a generalization of rateless codes is proposed. The proposed codes provide unequal error protection (UEP). The asymptotic properties of these codes under the iterative decoding are investigated. Moreover, upper and lower bounds on maximum-likelihood (ML) decoding error probabilities of finite-length LT and Raptor codes for both equal and unequal error protection schemes are derived. Further, our work is verified with simulations. Simulation results indicate that the proposed codes provide desirable UEP. We also note that the UEP property does not impose a considerable drawback on the overall performance of the codes. Moreover, we discuss that the proposed codes can provide unequal recovery time (URT). This means that given a target bit error rate, different parts of information bits can be decoded after receiving different amounts of encoded bits. This implies that the information bits can be recovered in a progressive manner. This URT property may be used for sequential data recovery in video/audio streaming [J525]

"South Korea's Way to the Future"

South Korea leads the world in access to broadband services; as of early 2006, 83 percent of households had broadband, compared to roughly 45 percent in the US. Not coincidentally, the country also leads in the transition to digital music sales via digital rights management (DRM) software. In fact; the past decade has seen South Korea's music scene change dramatically. It once had 8,000 music stores; now, it has 400-partly because of the Asian financial crisis of the late 1990s, but mostly due to the change in music distribution patterns. South Korea is also the first country in which online music sales exceeded CD sales in value. According to The Korea Times, South Koreans spent 400 billion won buying music from traditional stores in 1999; by 2005, that number was down to 108 billion won whereas online music purchases had reached 262 billion won. The exchange rate is roughly 1,000 won to every US dollar, so converting the word "billion" to "million" gives US readers an idea of what's going on in a country one-sixth the US s size and with 1 /15th of its gross domestic product. A typical South Korean mobile phone is a camera as well as a music player, and some include video players, stored value cards, and full keyboards. South Korea's ringtone market alone is larger than its CD market-ringtones brought in US$336 million in 2004, for example. Consumers can buy unlimited music downloads for $5 per month or broadband service for $20 per month-and they're about to have a new form of interoperability among music vendors [J526]

"Intelligent-Based Approach to Islanding Detection in Distributed Generation"

This paper introduces a new intelligent-based approach for detecting islanding in distributed generation (DG). This approach utilizes and combines various system parameter indices in order to secure the detection of islanding for any possible network topology, penetration level and operating condition of the DG under study. Hence, every parameter index displays characteristics for a given set of events. The proposed technique uses the data-mining technology to extract information from the large data sets of these indices after they are screened off-line via massive event analyses using network simulations. The technique is tested on a typical DG with multiple distributed resources and the results indicate that this technique can successfully detect islanding operations. In addition, this technique can also overcome the problem of setting the detection thresholds inherent in the existing techniques by optimizing their settings [J527]

"Setting Boundaries at Borders: Reconciling Laptop Searches and Privacy"

If you've traveled internationally on business, the odds are that you've taken your laptop with you. Like most

business travelers, you need these ubiquitous devices to do work, make presentations, and communicate with coworkers, family, and friends via the Internet. In a previous department, we explored the notion that laptops deserve special consideration because of the increasingly blurred line between home and office, the entrusting of intimate, private information to storage on laptops, and the resulting need to rethink the rules surrounding reasons-able expectations of privacy. This time, we examine the nexus between laptops, a government's search and seizure powers, and a traveler's transit through an international border checkpoint where customs officials have enhanced powers to search travelers and their belongings [J528]

"Implementation of the DLNA Proxy System for Sharing Home Media Contents"

The paper proposes a methodology to provide services for accessing and sharing various media contents securely, those are distributed over consumer electronics (CEs) in the home network. To do so, we propose the DLNA proxy system (DPS) architecture which helps to gather various media information available from the distributed AV devices in the home and to share the media contents across the public IP network via established secure channels. The proxy system is implemented on the home server which acts as media server and the hardware accelerated IP security (IPSec) virtual private network (VPN) is configured on the home gateway which establishes and maintains secure connections between the home and public networks [J529]

"Trust Negotiation in Identity Management"

Most organizations require the verification of personal information before providing services, and the privacy of such information is of growing concern. The authors show how federated identity management systems can better protect users' information when integrated with trust negotiation. In today's increasingly competitive business environment, more and more leading organizations are building Web-based infrastructures to gain the strategic advantages of collaborative networking. However, to facilitate collaboration and fully exploit such infrastructures, organizations must identify each user in the collaborative network as well as the resources each user is authorized to access. User identification and access control must be carried out so as to maximize user convenience and privacy without increasing organizations1 operational costs. A federation can serve as the basic context for determining suitable solutions to this issue. A federation is a set of organizations that establish trust relationships with respect to the identity information-the federated identity information-that is considered valid. A federated identity management system (idM) provides a group of organizations that collaborate with mechanisms for managing and gaining access to user identity information and other resources across organizational boundaries [J530]

"On Finding Feasible Solutions With Shared Backup Resources for Surviving Double-Link Failures in Path-Protected WDM Mesh Networks"

In this paper, we investigate the problem of dynamic survivable routing in wavelength-division-multiplexing optical networks and propose a new path-protection algorithm called Enhanced Shared Backup Paths Protection (ESBPP) to provide the complete survivability for double-link failures. In order to improve the resource-utilization ratio, we present the new rule of sharing backup resources that can yield better resource-utilization ratio than previous methods. In order to overcome the problem of trap paths, we develop a new routing method to find the feasible solution with three link-disjoint paths for each connection request. Compared to previous algorithms for double-link failures, ESBPP can obtain higher resource-utilization ratio and lower blocking probability [J531]

"An Accurate, Continuous, and Lossless Self-Learning CMOS Current-Sensing Scheme for Inductor-Based DC-DC Converters"

Sensing current is a fundamental function in power supply circuits, especially as it generally applies to protection and feedback control. Emerging state-of-the-art switching supplies, in fact, are now exploring ways to use this sensed-current information to improve transient response, power efficiency, and compensation performance by appropriately self-adjusting, on the fly, frequency, inductor ripple current, switching configuration (e.g., synchronous to/from asynchronous), and other operating parameters. The discontinuous, non-integrated, and inaccurate nature of existing lossless current-sensing schemes, however, impedes their widespread adoption, and lossy solutions are not acceptable. Lossless, filter-based techniques are continuous, but inaccurate when integrated on-chip because of the inherent mismatches between the filter and the power inductor. The proposed GM-C filter-based, fully integrated current-sensing CMOS scheme circumvents this accuracy limitation by introducing a self-learning sequence to start-up and power-on-reset. During these seldom-occurring events, the gain and bandwidth of the internal filter are matched to the response of the power inductor and its equivalent series resistance (ESR), effectively measuring their values. A 0.5 mum CMOS realization of the proposed scheme was fabricated and applied to a current-mode buck switching supply, achieving overall DC and AC current-gain errors of 8% and 9%, respectively, at 0.8 A DC load and 0.2 A ripple currents for 3.5 muH-14 muH

inductors with ESRs ranging from 48 mOmega to 384 mOmega (other lossless, state-of-the-art solutions achieve 20%-40% error, and only when the nominal specifications of the power MOSFET and/or inductor are known). Since the self-learning sequence is non-recurring, the power losses associated with the foregoing solution are minimal, translating to a 2.6% power efficiency savings when compared to the more traditional but accurate series-sense resistor (e.g., 50 mOm- ega) technique. [J532]

"Comments on "On Hamiltonian Cycles as Optimal p-Cycles""

For original paper by D.A. Schupke see ibid., vol.9, no 4, p.360-2, April 2005. It is shown that in the above letter by Schupke corollaries related to a necessary condition on the network to ensure that a set of Hamiltonian p-cycles is able to reach the theoretical logical redundancy bound are wrongly calculated [J533]

"Convolutional and Tail-Biting Quantum Error-Correcting Codes"

Rate-(n-2)/n unrestricted and CSS-type quantum convolutional codes with up to 4096 states and minimum distances up to 10 are constructed as stabilizer codes from classical self-orthogonal rate-1/n F4-linear and binary linear convolutional codes, respectively. These codes generally have higher rate and less decoding complexity than comparable quantum block codes or previous quantum convolutional codes. Rate-(n-2)/n block stabilizer codes with the same rate and error-correction capability and essentially the same decoding complexity are derived from these convolutional codes via tail-biting [J534]

"Defense Against Spoofed IP Traffic Using Hop-Count Filtering"

IP spoofing has often been exploited by Distributed Denial of Service (DDoS) attacks to: 1)conceal flooding sources and dilute localities in flooding traffic, and 2)coax legitimate hosts into becoming reflectors, redirecting and amplifying flooding traffic. Thus, the ability to filter spoofed IP packets near victim servers is essential to their own protection and prevention of becoming involuntary DoS reflectors. Although an attacker can forge any field in the IP header, he cannot falsify the number of hops an IP packet takes to reach its destination. More importantly, since the hop-count values are diverse, an attacker cannot randomly spoof IP addresses while maintaining consistent hop-counts. On the other hand, an Internet server can easily infer the hop-count information from the Time-to-Live (TTL) field of the IP header. Using a mapping between IP addresses and their hop-counts, the server can distinguish spoofed IP packets from legitimate ones. Based on this observation, we present a novel filtering technique, called Hop-Count Filtering (HCF)-which builds an accurate IP-to-hop-count (IP2HC) mapping table-to detect and discard spoofed IP packets. HCF is easy to deploy, as it does not require any support from the underlying network. Through analysis using network measurement data, we show that HCF can identify close to 90% of spoofed IP packets, and then discard them with little collateral damage. We implement and evaluate HCF in the Linux kernel, demonstrating its effectiveness with experimental measurements [J535]

"Adaptive Distance Relay Setting for Lines Connecting Wind Farms"

Wind speed varies continuously throughout a day resulting in fluctuating wind farm output power. When such a farm is connected to the grid through a line, the transmitted power and the relay end voltage (with respect to grid voltage) fluctuate continuously. In this paper, the protection of such a line with distance relay is investigated. The ideal trip characteristic for distance relay is studied with change in conditions of the wind farm. A method is proposed to set the boundary adaptively using local information only [J536]

"Taking a Hard-Line Approach to Encryption"

Information security during the past few years has concentrated largely on data in motion-information communicated via networks. However, the focus has been shifting recently to protecting data at rest, which includes information on hard drives, flash memory devices, and magnetic tape. Over time, the technology in encryption-enabled hard drives is likely to change. Drives could increasingly include TCG technology or use new types of encryption as they are developed [J537]

"Privacy and security as ideology"

Privacy and data protection are among the prime problems of the information society. The terms privacy and security promotes a particular ideology and uses the ethical recognition of the concepts to limit critical discourses. This article uses a critical approach in the tradition of critical theory and its developments in critical research in information systems (CRIS) to expose and overcome these discursive closures. The author begins with a review of the literature on privacy and security, which will support the contention that these are ethical concepts. The concept of ideology and critical research is discussed. This will lead to a critical discourse analysis

of a text from a commercial software vendor, which will provide empirical evidence of the ideological use of the terms privacy and security [J538]

"An Automatically Tuning Intrusion Detection System"

An intrusion detection system (IDS) is a security layer used to detect ongoing intrusive activities in information systems. Traditionally, intrusion detection relies on extensive knowledge of security experts, in particular, on their familiarity with the computer system to be protected. To reduce this dependence, various data-mining and machine learning techniques have been deployed for intrusion detection. An IDS is usually working in a dynamically changing environment, which forces continuous tuning of the intrusion detection model, in order to maintain sufficient performance. The manual tuning process required by current systems depends on the system operators in working out the tuning solution and in integrating it into the detection model. In this paper, an automatically tuning IDS (ATIDS) is presented. The proposed system will automatically tune the detection model on-the-fly according to the feedback provided by the system operator when false predictions are encountered. The system is evaluated using the KDDCup'99 intrusion detection dataset. Experimental results show that the system achieves up to 35% improvement in terms of misclassification cost when compared with a system lacking the tuning feature. If only 10% false predictions are used to tune the model, the system still achieves about 30% improvement. Moreover, when tuning is not delayed too long, the system can achieve about 20% improvement, with only 1.3% of the false predictions used to tune the model. The results of the experiments show that a practical system can be built based on ATIDS: system operators can focus on verification of predictions with low confidence, as only those predictions determined to be false will be used to tune the detection model [J539]

"A Fully Distributed Proactively Secure Threshold-Multisignature Scheme"

Threshold-multisignature schemes combine the properties of threshold group-oriented signature schemes and multisignature schemes to yield a signature scheme that allows a threshold (t) or more group members to collaboratively sign an arbitrary message. In contrast to threshold group signatures, the individual signers do not remain anonymous, but are publicly identifiable from the information contained in the valid threshold-multisignature. The main objective of this paper is to propose such a secure and efficient threshold-multisignature scheme. The paper uniquely defines the fundamental properties of threshold-multisignature schemes and shows that the proposed scheme satisfies these properties and eliminates the latest attacks to which other similar schemes are subject. The efficiency of the proposed scheme is analyzed and shown to be superior to its counterparts. The paper also proposes a discrete logarithm based distributed-key management infrastructure (DKMI), which consists of a round optimal, publicly verifiable, distributed-key generation (DKG) protocol and a one round, publicly verifiable, distributed-key redistribution/ updating (DKRU) protocol. The round optimal DKRU protocol solves a major problem with existing secret redistribution/updating schemes by giving group members a mechanism to identify malicious or faulty share holders in the first round, thus avoiding multiple protocol executions [J540]

"P3P Adoption on E-Commerce Web sites: A Survey and Analysis"

Privacy is an increasingly important issue for Internet users, especially in the world of e-commerce, where they must disclose large amounts of personal information to make purchases. Various privacy-enhancing technologies (PETs) are currently available, including the platform for privacy preferences project, privacy seals, and human-readable privacy policies. In particular, P3P has been the subject of considerable interest; however, it's also highly dependent on the symbiotic deployment of P3P user agents and policies on vendors' Web sites. Internet users and vendors must commit time and resources to deploy P3P agents or policies, and thus require evidence that the technology won't stagnate or become obsolete. In this article, we survey the current rate of P3P deployment within the e-commerce industry. We also examine P3P's usefulness as a PET, using Everett Rogers' drivers of innovation adoption [J541]

"Joint Source-Channel Rate Allocation in Parallel Channels"

A fast rate-optimal rate allocation algorithm is proposed for parallel transmission of scalable images in multichannel systems. Scalable images are transmitted via fixed-length packets. The proposed algorithm selects a subchannel, as well as a channel code rate for each packet, based on the signal-to-noise ratios (SNRs) of the subchannels. The resulting scheme provides unequal error protection of source bits and significant gains are obtained over equal error protection schemes. An application of the proposed algorithm to JPEG2000 transmission shows the advantages of exploiting differences in SNRs between subchannels. Multiplexing of multiple sources is also considered, and additional gains are achieved by exploiting information diversity among the sources. [J542]

"Collusion-Resistant Video Fingerprinting for Large User Group"

Digital fingerprinting protects multimedia content from illegal redistribution by uniquely marking copies of the content distributed to users. Most existing multimedia fingerprinting schemes consider a user set on the scale of thousands. However, in such real-world applications as video-on-demand distribution, the number of potential users can be as many as 10-100 million. This large user size demands not only strong collusion resistance but also high efficiency in fingerprint construction, and detection, which makes most existing schemes incapable of being applied to these applications. A recently proposed joint coding and embedding fingerprinting framework provides a promising balance between collusion resistance, efficient construction, and detection, but several issues remain unsolved for applications involving a large group of users. In this paper, we explore how to employ the joint coding and embedding framework and develop practical algorithms to fingerprint video in such challenging settings as to accommodate more than ten million users and resist hundreds of users' collusion. We investigate the proper code structure for large-scale fingerprinting and propose a trimming detection technique that can reduce the decoding computational complexity by more than three orders of magnitude at the cost of less than 0.5% loss in detection probability under moderate to high watermark-to-noise ratios. Both analytic and experimental results show a high potential of joint coding and embedding to meet the needs of real-world large-scale fingerprinting applications. [J543]

"Fingerprint-Based Fuzzy Vault: Implementation and Performance"

Reliable information security mechanisms are required to combat the rising magnitude of identity theft in our society. While cryptography is a powerful tool to achieve information security, one of the main challenges in cryptosystems is to maintain the secrecy of the cryptographic keys. Though biometric authentication can be used to ensure that only the legitimate user has access to the secret keys, a biometric system itself is vulnerable to a number of threats. A critical issue in biometric systems is to protect the template of a user which is typically stored in a database or a smart card. The fuzzy vault construct is a biometric cryptosystem that secures both the secret key and the biometric template by binding them within a cryptographic framework. We present a fully automatic implementation of the fuzzy vault scheme based on fingerprint minutiae. Since the fuzzy vault stores only a transformed version of the template, aligning the query fingerprint with the template is a challenging task. We extract high curvature points derived from the fingerprint orientation field and use them as helper data to align the template and query minutiae. The helper data itself do not leak any information about the minutiae template, yet contain sufficient information to align the template and query fingerprints accurately. Further, we apply a minutiae matcher during decoding to account for nonlinear distortion and this leads to significant improvement in the genuine accept rate. We demonstrate the performance of the vault implementation on two different fingerprint databases. We also show that performance improvement can be achieved by using multiple fingerprint impressions during enrollment and verification. [J544]

"Google, Profiling, and Privacy"

Antitrust questions put a useful spotlight on the privacy issues of online profiling by those who sell advertising on the Web. These questions apply not just to Google but to any site that uses personal information and behavior data to develop and use individual users' profiles. But simply assuring advertisers a fair marketplace won't be sufficient to guarantee user privacy. We know that many users are willing to give up some privacy protection for short-term convenience, but we shouldn't conclude from these chokes that privacy means the sum total of whatever people end up choosing. [J545]

"Selective Error Detection for Error-Resilient Wavelet-Based Image Coding"

This paper introduces the concept of a similarity check function for error-resilient multimedia data transmission. The proposed similarity check function provides information about the effects of corrupted data on the quality of the reconstructed image. The degree of data corruption is measured by the similarity check function at the receiver, without explicit knowledge of the original source data. The design of a perceptual similarity check function is presented for wavelet-based coders such as the JPEG2000 standard, and used with a proposed ldquoprogressive similarity-based ARQrdquo (ProS-ARQ) scheme to significantly decrease the retransmission rate of corrupted data while maintaining very good visual quality of images transmitted over noisy channels. Simulation results with JPEG2000-coded images transmitted over the binary symmetric channel, show that the proposed ProS-ARQ scheme significantly reduces the number of retransmissions as compared to conventional ARQ-based schemes. The presented results also show that, for the same number of retransmitted data packets, the proposed ProS-ARQ scheme can achieve significantly higher PSNR and better visual quality as compared to the selective-repeat ARQ scheme. [J546]

"Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation

of Security Threats"

The Internet has become a wild place: malicious code is spread on personal computers across the world, deploying botnets ready to attack the network infrastructure. The vast number of security incidents and other anomalies overwhelms attempts at manual analysis, especially when monitoring service provider backbone links. We present an approach to interactive visualization with a case study indicating that interactive visualization can be applied to gain more insight into these large data sets. We superimpose a hierarchy on IP address space, and study the suitability of Treemap variants for each hierarchy level. Because viewing the whole IP hierarchy at once is not practical for most tasks, we evaluate layout stability when eliding large parts of the hierarchy, while maintaining the visibility and ordering of the data of interest. [J547]

"Protecting a High Horsepower Motor"

Protecting the motor is obviously the most important task of protection relays regardless of the technology that they are based on. Microprocessor-based relays are capable of processing the measured data (i.e., current, voltage, and status indication) in many different ways. Registered data in the relay can be sent through a communication network to the operation/engineering headquarters for continuous monitoring or fault analysis. In addition to being used for motor protection, relays provide useful information to other departments (maintenance, planning, etc.). [J548]

"Enterprise Security for Web 2.0"

Web 2.0 is among the most talked-about, highest-buzz IT constructs of late, the subject of numerous articles and blogs and, since 2004, multiple conferences. While in many respects an Internet phenomenon, Web 2.0 is quickly gaining a beachhead against the legacy "stovepiped" way in which users manage and disseminate information of all kinds within the enterprise. It's also an outside-in revolution: Technologies developed and explored outside the enterprise are migrating inside it. People who've gotten hooked on Web 2.0 demand the same user experience, tools, and networking in their work that they've experienced at play. The good news for enterprise security practitioners is that the impact of Web 2.0 has thus far been evolutionary. However, Web 2.0 growth is accelerating, and it's doing so for reasons as varied as compliance, privacy, and protection of corporate assets. Organizations considering deployment of Web 2.0 capabilities must exercise caution and control, just as they do with non-Web 2.0 technologies. What's needed, in short, is Security 2.0. [J549]

"Performance Analysis of a Coherent FH-MA System Based on Latin Squares"

Frequency hopping (FH) combined with coding is a popular technique in wireless communication applications. Motivated by the commercial system outlined in [1], this paper investigates the performance of a coherent FH multiple access (FH-MA) cellular system, where hopping patterns are constructed from latin squares. Some of the patterns carry pilot symbols, which the users track to estimate the channel on the data patterns and perform coherent detection. The latin squares construction enables us to analytically evaluate the bit error probability (BEP) over each data pattern, when convolutional codes are employed for error protection. The focus of our work is to precisely determine the effect that frequency and interference diversity, ensuing from FH, have on the coded performance. Regarding frequency diversity, it is shown that the performance can vary widely for different latin squares. Moreover, under pilot-assisted channel estimation, a performance tradeoff is observed, as an increasing frequency selectivity results in more diversity, but also more inaccurate channel state information. With respect to interference diversity, we analyze the performance when the interference power variations are perfectly known or ignored by the receiver. Our results confirm that interference tracking is important in harnessing the error correcting power of convolutional coding. [J550]

"Practical Minimalist Cryptography for RFID Privacy"

The fear of unauthorized, hidden readouts has dominated the radio frequency identification (RFID) privacy debate. Virtually all proposed privacy mechanisms so far require consumers to actively and explicitly protect read access to their tagged items-either by jamming rogue readers or by encrypting or pseudonymizing their tags. While this approach might work well for activists and highly concerned individuals, it is unlikely (and rather undesirable) that the average consumer should be outfitted with RFID jamming devices before stepping outside, or that anyone would bother pseudonymizing every can of soda they buy with a personal PIN code. Juels' ldquominimalist cryptographyrdquo offers a simple, yet effective, identification and tracking protection based on simple ID rotation, but it requires that the corresponding mappings (i.e., from pseudonyms to real IDs) are electronically exchanged whenever a product changes hands (e.g., for buying a pack of chewing gum at a kiosk)-a rather impractical requirement. Our work extends Juels' concept in order to alleviate the need for passing ID mapping tables. Using carefully assembled sets of IDs based on the cryptographic principle of secret shares, we can create RFID tags that yield virtually no information to casual ldquohit-and-runrdquo attackers, but

only reveal their true ID after continuous and undisturbed reading from up-close-something that can hardly go unnoticed by an item's owner. This paper introduces the underlying mechanism of our extension to Juels' proposal, called ldquoShamir Tag,rdquo analyzes its tracking resistance and identification performance, and discusses deployment aspects. [J551]

"Optimum Detection for Spread-Spectrum Watermarking That Employs Self-Masking"

Digital watermarking is an efficient and promising approach to protect intellectual property rights of digital media. Spread spectrum (SS) is one of the most widely used image watermarking schemes because of its robustness against attacks and its support for the exploitation of the properties of the human visual system (HVS). To maximize the watermark strength without introducing visual artifacts, in SS watermarking, the watermark signal is usually modulated by the just-noticeable difference (JND) of the host image. In advanced perceptual models, the JND is characterized as a nonlinear function of local image features. The optimum detection scheme for such nonlinearly embedded watermarks, however, has rarely been studied. In this paper, we address this problem and propose a novel approach that transforms the test signal to a perceptually uniform domain and then performs Bayesian hypothesis testing in that domain. Locally optimum detectors for arbitrary host signal distributions and arbitrary JND models that exploit the self-masking property of the HVS are derived in closed forms, in which the test signal is first nonlinearly preprocessed before a linear correlator is applied. The optimality of the proposed detector is justified mathematically according to the Neyman-Pearson criterion. Simulation results demonstrate the superior performances of the proposed detector over the conventional linear correlation detector. [J552]

"Undervoltage Load Shedding Using Distributed Controllers"

A new load shedding scheme against long-term voltage instability is proposed. It uses a set of distributed controllers, each monitoring transmission voltages in a zone and controlling a group of related loads. Each controller acts in closed-loop, shedding amounts that vary in magnitude and time according to the evolution of its monitored voltage. The whole system can operate without information exchange between controllers, the latter being implicitly coordinated through network voltages. The operation, design and robustness features are illustrated through simulations of a real system. [J553]

"Distributed Undervoltage Load Shedding"

A new design of load shedding against long-term voltage instability is proposed. It uses a set of distributed controllers, each monitoring a transmission voltage, controlling a group of loads, acting in closed-loop, and adjusting its action to the voltage evolution. The whole system operates without information exchange between controllers. [J554]

"Security and Privacy in Pervasive Computing"

In this issue's Works in Progress department, we have six projects. The first two projects address an individual's privacy concerns and preferences. The next entry discusses a project on data protection for electronic passports. The remaining three projects are investigating various types of privacy protection mechanisms for data collected in pervasive computing environments, by attestation services, and by voice recording systems. [J555]

"A Comparison of Collaborative-Filtering Recommendation Algorithms for E-commerce"

Collaborative filtering is one of the most widely adopted and successful recommendation approaches. Unlike approaches based on intrinsic consumer and product characteristics, CF characterizes consumers and products implicitly by their previous interactions. The simplest example is to recommend the most popular products to all consumers. Researchers are advancing CF technologies in such areas as algorithm design, human- computer interaction design, consumer incentive analysis, and privacy protection. [J556]

"Physical Access Control for Captured RFID Data"

To protect the privacy of RFID data after an authorized system captures it, this policy-based approach constrains the data users can access to system events that occurred when and where they were physically present. RFID security is a vibrant research area, with many protection mechanisms against unauthorized RFID cloning and reading attacks emerging. However, little work has yet addressed the complementary issue of protecting the privacy of RFID data after an authorized system has captured and stored it. We've investigated peer-to-peer privacy for personal RFID data through an access-control policy called Physical Access Control. PAC protects privacy by constraining the data a user can obtain from the system to those events that occurred when and where that user was physically present. While strictly limiting information disclosure, PAC also affords a database view that augments users' memory of places, objects, and people. PAC is appropriate as a default

level of access control because it models the physical boundaries in everyday life. Here, we focus on the privacy, utility, and security issues raised by its implementation in the RFID Ecosystem. [J557]

"Decode-Time Forensic Watermarking of AAC Bitstreams"

In digital rights-management systems, forensic watermarking complements encryption and deters the capture and unauthorized redistribution of the rendered content. In this paper, we propose a novel watermarking method which is integrated into the advanced audio coding (AAC) standard's decoding process. For predefined frequency bands, the method intercepts and modifies the scale factors, which are utilized for dequantization of spectral coefficients. It thereby modulates the short-time envelope of the bandlimited audio and embeds a watermark which is robust to various attacks, such as capture with a microphone and recompression at lower bit rates. Inclusion of watermark embedding in the AAC decoder has practically no effect on the decoding complexity. As a result, the proposed method can be integrated even into resource-constrained devices, such as portable players without any additional hardware. [J558]

"Multiplicative Linear Secret Sharing Schemes Based on Connectivity of Graphs"

The multiplicative property is important for a linear secret sharing scheme (LSSS) to be used in constructing a multiparty computation (MPC) protocol. In general, an LSSS has to expand its share size to obtain the multiplicative property. In this paper, with respect to an MPC problem based on connectivity of graphs we devise an ideal multiplicative LSSS, that is, the LSSS is of the multiplicative property without expanding its share size. Moreover, it provides a new class of access structures that have ideal multiplicative LSSSs. [J559]

"Distortion-Driven Video Streaming over Multihop Wireless Networks with Path Diversity"

Multihop networks provide a flexible infrastructure that is based on a mixture of existing access points and stations interconnected via wireless links. These networks present some unique challenges for video streaming applications due to the inherent infrastructure unreliability. In this paper, we address the problem of robust video streaming in multihop networks by relying on delay- constrained and distortion-aware scheduling, path diversity, and retransmission of important video packets over multiple links to maximize the received video quality at the destination node. To provide an analytical study of this streaming problem, we focus on an elementary multihop network topology that enables path diversity, which we term "elementary cell." Our analysis is considering several cross-layer parameters at the physical and medium access control (MAC) layers, as well as application-layer parameters such as the expected distortion reduction of each video packet and the packet scheduling via an overlay network infrastructure. In addition, we study the optimal deployment of path diversity in order to cope with link failures. The analysis is validated in each case by simulation results with the elementary cell topology, as well as with a larger multihop network topology. Based on the derived results, we are able to establish the benefits of using path diversity in video streaming over multihop networks, as well as to identify the cases where path diversity does not lead to performance improvements. [J560]

"Expert Systems for Earthquake Damage Assessment"

An earthquake is a calamity that can cause colossal damage to buildings, infrastructure, and environment, consequently leading to heavy casualties. It is therefore imperative for disaster relief agencies and civil protection bodies to assess the damage for planning purposes. Satellite remote sensing and geographic information systems can help prepare initial damage assessment maps. This examines the preparation of damage assessment maps using decision tree-based expert systems. The inductive machine learning-based decision tree classification has correctly identified 61% of the severely damaged buildings, and hence, is a viable option for preparing damage assessment maps. [J561]

"Analysis of Errors and Erasures in Parity Sharing RS Codecs"

Reed Solomon (RS) codes are widely used to protect information from errors in transmission and storage systems. Most of the RS codes are based on GF(28) Galois Fields and use a byte to encode a symbol providing codewords up to 255 symbols. Codewords with more than 255 symbols can be obtained by using GF(2m) Galois fields with m > 8, but this choice increases the complexity of the encoding and decoding algorithms. This limitation can be superseded by introducing parity sharing (PS) RS codes that are characterized by a greater flexibility in terms of design parameters. Consequently, a designer can choose between different PS code implementations in order to meet requirements such as bit error rate (BER), hardware complexity, speed, and throughput. This paper analyzes the performance of PS codes in terms of BER with respect to the code parameters, taking into account either random error or erasure rates as two independent probabilities. This approach provides an evaluation that is independent of the communication channel characteristics and extends the results to memory systems in which permanent faults and transient faults can be modeled, respectively, as

erasures and random errors. The paper also provides hardware implementations of the PS encoder and decoder and discusses their performances in terms of hardware complexity, speed, and throughput. [J562]

"On the Trustworthiness of Error-Correcting Codes"

The use of error-correcting codes protects data against accidental or intentional errors, but to what extent can a decoded message be trusted? To answer this question, one has to take the role of the receiver. First, the maximum number of errors Lambda acceptable for decoding is fixed. With the weight distribution, the probability of false decoding can be calculated, conditioned on such a Lambda-bounded strategy. This probability is a monotonously increasing function in the channel error probability p and in the maximum number of accepted errors Lambda. Therefore, pure error detection is more trustworthy than error correction. Moreover, for sufficiently small p, codes with the lexicographically smallest weight distribution prove to be most trustworthy. An example of how to calculate and use the probability of false decoding is given in the context of the pseudonymization service of the German telematics platform TMF for health research networks. [J563]

"E-Passport Threats"

The International Civil Aviation Organization (ICAO) standardized e-passports by specifying how to implement and protect machine-readable travel documents. E-passports have embedded contactless chips that can be read by radio from tip to a few centimeters away. The ICAO chose this technology over magnetic strips and 2D barcodes because it provides reliable connection, large memory capacity, random access, and rewritable memory. As with many other RFID devices, the chip in e-passports uses a 32-bit number for collision avoidance. Every country maintains its own public-key infrastructure (PKI) and exchanges root certificates with other countries via diplomatic means. Agencies issuing e-passports have their own public keys and certificates from the PKI. In this way, a passive authentication mechanism verifies every data group's digest. With today's e-passports, private information is limited to the MRZ and a digital picture, but the goal is to eventually add more biometrics at some point, along with a digitized handwritten signature. [J564]

"Who Are the Experts, and What Have They Done for Us Lately?"

Gaining the recognition for the security and privacy field as an assemblage of experts requires more than a simple assertion of expertise and a declaration of standards. We must be able to objectively assess our own performance, individually and as a whole, and determine if we are, as a field, improving computer security. [J565]

"Developing a Culture of Privacy: A Case Study"

In building a culture of privacy, an organization must clearly articulate privacy as an organizational priority; communicate key privacy and security messages; educate across the organization; raise awareness of the importance of registering privacy incidents and breaches; build privacy into the fabric of the organization's activities; and make privacy information and guidance readily accessible. Accomplishing these objectives provides a framework to create or reinforce a privacy culture. In 2003, the province of Ontario, Canada, created the smart systems for health agency (SSHA) to connect healthcare professionals across the province. [J566]

"Web Camouflage: Protecting Your Clients from Browser-Sniffing Attacks"

Browser cache and history are intended to be private, yet it's not difficult for malicious Web sites to "sniff" cache entries on visitors' computers and then use that information to more accurately deceive them. The authors' approach neutralizes the threat of URLs being discovered on client computers. [J567]

"Lessons from the Norwegian ATM System"

This case study focuses on real-world ATM card misuse, illustrating how too much secrecy led to a deterioration of PIN-based authentication procedures, and why a bank's refusal to share technical information is a threat to customers during a conflict. [J568]

"Overcurrent Protection in Electrical Distribution Systems Through Probabilistic Approach"

This work describes the study of distribution system overcurrent protection through a probabilistic approach. Conventional approaches for overcurrent protection do not consider the probabilistic nature of the main variables involved, such as fault location, fault type and fault impedance for faults involving the ground. In this case, for instance, it is very difficult to assess the impact of situations where full coordination cannot be attained for some reason. The probabilistic approach, on the other hand, allows quantifying the risk of two adjacent protective

devices operating in a non-coordinated way. This information is extremely valuable for electrical engineers at design level. In this work, the proposed methodology is illustrated through a few detailed application studies, including various sensitivity analyzes for assessing the influence of model parameters on the coordination of protective devices. [J569]

"Key management requirements for PTC operations"

Positive train control (PTC) is an electronic system that enforces activities such as train separation, speed enforcement, and roadway worker protection essential to operate railroads safely and efficiently. Vehicular ad-hoc networks (VANETS) provide distributed real time communication of traffic hazards and road conditions among vehicles in a radio line of sight. Communicating PTC VANET systems offer the potential to reduce highway rail intersection (HRI) collisions by communicating train movement information to highway vehicles. For this to occur, different PTC systems must securely interoperate with each other. This outlines a PTC security framework utilizing using a certificate based trust management system and over the air re-keying (OTAR) to support interoperation. [J570]

"Where Does Security Stand? New Vulnerabilities vs. Trusted Computing"

How can we ensure that platform hardware, firmware, and software work in concert to withstand rapidly evolving security threats? Architectural innovations bring performance gains but can also create new security vulnerabilities. In this panel discussion, from the 2007 workshop on Computer Architecture Research directions, we assess the current state of security and discuss possible routes toward trusted computing. [J571]

"About Penetration Testing"

Students generally learn red teaming, sometimes called penetration testing or ethical hacking, as "breaking into your own system to see how hard it is to do so". Contrary to this simplistic view, a penetration test requires a detailed analysis of the threats and potential attackers in order to be most valuable. Using the results of penetration testing requires proper interpretation. Neither testers nor sponsors should assert that the penetration test has found all possible flaws, or that the failure to find flaws means that the system is secure. All types of testing can show only the presence of flaws and never the absence of them. The best that testers can say is that the specific flaws they looked for and failed to find aren't present: this can give some idea of the overall security of the system's design and implementation. [J572]

"Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks"

To proactively defend against intruders from readily jeopardizing single-path data sessions, we propose a distributed secure multipath solution to route data across multiple paths so that intruders require much more resources to mount successful attacks. Our work exhibits several important properties that include: (1) routing decisions are made locally by network nodes without the centralized information of the entire network topology; (2) routing decisions minimize throughput loss under a single-link attack with respect to different session models; and (3) routing decisions address multiple link attacks via lexicographic optimization. We devise two algorithms termed the Bound-Control algorithm and the Lex-Control algorithm, both of which provide provably optimal solutions. Experiments show that the Bound-Control algorithm is more effective to prevent the worst-case single-link attack when compared to the single-path approach, and that the Lex-Control algorithm further enhances the Bound-Control algorithm by countering severe single-link attacks and various types of multi-link attacks. Moreover, the Lex-Control algorithm offers prominent protection after only a few execution rounds, implying that we can sacrifice minimal routing protection for significantly improved algorithm performance. Finally, we examine the applicability of our proposed algorithms in a specialized defensive network architecture called the attack-resistant network and analyze how the algorithms address resiliency and security in different network settings. [J573]

"Intrusion detection techniques in mobile ad hoc and wireless sensor networks"

Mobile ad hoc networks and wireless sensor networks have promised a wide variety of applications. However, they are often deployed in potentially adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. Intrusion detection systems provide a necessary layer of in-depth protection for wired networks. However, relatively little research has been performed about intrusion detection in the areas of mobile ad hoc networks and wireless sensor networks. In this article, first we briefly introduce mobile ad hoc networks and wireless sensor networks and their security concerns. Then, we focus on their intrusion detection capabilities. Specifically, we present the challenge of constructing intrusion detection systems for mobile ad hoc networks and wireless sensor networks, survey the existing intrusion detection techniques, and indicate important future research directions. [J574]

"Guest Editors' Introduction: Security and Trust in Embedded-Systems Design"

Security and trust have become important considerations in the design of virtually all modern embedded systems. The requirements of secure and trusted design are unique: Secure design emphasizes information leakage (or prevention thereof) and dependable behavior. Even strong cryptographic algorithms are of little use if the underlying processor can be tricked into releasing cryptographic keys. This leads to unique design techniques such as design and implementation of boundaries for logical and physical protection, design of protected storage and secure-computing primitives, runtime measurement and reporting of security properties, and implementation of side-channel-resistant hardware and software. Eventually, the embedded-system designer must cope with security as yet another requirement in addition to existing functional requirements, performance, power, and cost. This special issue presents six articles that address various critical aspects of secure embedded-systems design. [J575]

"A design for secure and survivable wireless sensor networks"

In this article, we present a study of the design of secure and survivable wireless sensor networks (WSN) that has yet to be addressed in the literature. Our goal is to develop a framework that provides the security and survivability features that are crucial to applications in a WSN, because WSNs are vulnerable to physical and network-based security attacks, accidents, and failures. To achieve such a goal, we first examine the security and survivability requirements. We then propose a security and survivability architecture in a WSN with heterogeneous sensor nodes. To understand the interactions between survivability and security, we also design and analyze a key management scheme. The results of the experiment show that a good design can improve both security and survivability of a WSN; however, in some situations, there is a trade off between security and survivability. [J576]

"Achieving Shared Protection for Dynamic Multicast Sessions in Survivable Mesh WDM Networks"

The advances in wavelength-division multiplexing (WDM) technology are expected to facilitate bandwidth-intensive multicast applications. A single fiber failure in such a network, however, can disrupt the information dissemination to several destination nodes in a "light-tree"-based multicast session. Thus it is imperative to protect the multicast sessions. In this paper, we propose a novel protection scheme, called multicast protection through spanning paths (MPSP), for resource efficient multicast protection with spare capacity sharing. Here, a spanning path is a path from a leaf node to any other leaf node of a multicast tree. The key idea of MPSP is first to identify a backup path for each spanning path and then to appropriately select parts of these backup paths to protect the primary multicast tree, so that the total bandwidth allocated to the primary multicast tree and its protection paths (or trees, etc.) is minimized. While previous studies only consider self-sharing and intra-request sharing, to the best of our knowledge, this is the first time to take inter-request sharing of spare capacity into consideration when protecting dynamic multicast sessions. We use simulations to demonstrate the performance of the MPSP scheme. It is shown that significant performance improvements are achieved in terms of average cost per multicast session and blocking probability. Compared with existing schemes, the average cost is reduced by about 22% and the blocking probability can be reduced by about 27% in average. [J577]

"Using Topology Aggregation for Efficient Shared Segment Protection Solutions in Multi-Domain Networks"

The dynamic routing problem for Overlapping Segment Shared Protection (OSSP) in multi-domain networks has not received a lot of interest so far as it is more complex than in single-domain networks. Difficulties lie in the lack of complete and global knowledge about network topologies and bandwidth allocation whereas this knowledge is easily available in single-domain networks. We propose a two-step routing approach for the OSSP based on a topology aggregation scheme and link cost estimation: an inter-domain step and an intra-domain step. We propose two different heuristics, GROS and DYPOS for the inter-domain step, and a "Blocking-go-back" strategy in order to reduce the blocking rate in the intra-domain step. We compare the performance of the two heuristics against an optimal single-domain approach. We show that both heuristics lead to resource efficient solutions that are not far from the optimal ones. Moreover, both heuristics require relatively small computational efforts and are scalable for multi-domain networks. [J578]

"Protecting Critical Data"

TrustZone technology provides a defense against malicious software attempting to tamper with critical data such as digital-rights management (DRM) counters. The basic premise of our solution is that the state of the flash can serve as a point of reference to detect when rollback has occurred. Our solution is embodied in a trusted software application that needs the protection provided by the TrustZone Secure World. This application

represents the flash's state by generating a hash over a 32-byte sample of contiguous flash content, starting at a randomly selected address. The reference hash of the critical data is retrieved by decrypting the stored items just described and reversing the process. Next, the critical data itself is decrypted, and a new hash is generated from it. The new hash is compared with the reference hash to determine the critical data's integrity. [J579]

"Security evaluation of certain broadcast encryption schemes employing a generalized time-memory-data trade-off"

In this letter a weakness of certain broadcast encryption schemes in which the protected delivery of a session key (SEK) is based on XOR-ing this SEK with the IDs of the keys employed for its encryption is addressed. The weakness can be effectively explored assuming passive attacking which in the cases corresponding to a malicious legitimate user being the attacker, is a ciphertext only attack. A dedicated algorithm for cryptanalysis is proposed based on a generalized time-memory-data trade-off approach and its main characteristics are derived. The developed algorithm points out a security weakness of employing a block cipher with block length shorter than the key length in the considered BE schemes. [J580]

"Security in SRAM FPGAs"

As FPGAs have grown larger and more complex, the value of the IP implemented in them has grown commensurately. Since SRAM FPGAs reload their programming data every time they are powered up, an adversary can potentially copy the program as it is being loaded. FPGA manufacturers have added security features to protect designs from unauthorized copy, theft, and reverse-engineering as the bitstream is transmitted from permanent storage into the FPGA. These bitstream security features use well-known information security methods to protect design data. In this discussion, it is assumed that an adversary has physical access to the FPGA. In this environment, denial-of-service attacks on the configuration are irrelevant: A trivial denial-of-service method would be to physically damage the device-the so-called "whack-it-with-a-hammer" attack. [J581]

"Power Analysis Attacks and Countermeasures"

This article focuses on power analysis attacks because they have received by far the most attention in recent years. They are powerful and can be executed relatively easily. This article provides an introduction to these attacks and discusses countermeasures against them. In particular, we focus on countermeasures that can be implemented at the cell level. This article presents an overview of power analysis attacks, which are based on the measurement of the power consumed by cryptographic ICs, and countermeasures against them. [J582]

"Faults, Injection Methods, and Fault Attacks"

An active attacker can induce errors during the computation of the cryptographic algorithm and exploit the faulty results to extract information about the secret key in embedded systems. We call this kind of attack a fault attack. Fault attacks can break an unprotected system more quickly than any other kind of side-channel attack such as simple power analysis (SPA), differential power analysis (DPA), or electromagnetic analysis (EMA). For example, the attacker can break RSA-CRT (RSA with Chinese Remainder Theorem) with one faulty result, and Data Encryption Standard (DES) and Advanced Encryption Standard (AES) with two. Furthermore, the protection of fault attacks is more costly in terms of chip area. Here, we survey fault injection methods, types of faults, and fault attack models. [J583]

"Protecting Transportation Infrastructure"

In the context of homeland security, critical infrastructures are "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security, or economic well-being of citizens or the effective functioning of governments." Transportation infrastructures are a key component of a nation's critical infrastructures, covering physical assets such as airports, ports, and railway and mass transit networks as well as software systems such as traffic control systems. In effect, among various critical infrastructures spanning a range of economic sectors and government operations, transportation is widely viewed as one of the most significant and impactful. A 2002 study concerning the significance of infrastructure components and the consequences of a destructive event rated transportation as "extremely significant." Other components at this highest level of significance were communications, power, emergency response personnel and assets, and national security resources. [J584]

"Keeping Denial-of-Service Attackers in the Dark"

We consider the problem of overcoming (distributed) denial-of-service (DoS) attacks by realistic adversaries that have knowledge of their attack's successfulness, for example, by observing service performance degradation or

by eavesdropping on messages or parts thereof. A solution for this problem in a high-speed network environment necessitates lightweight mechanisms for differentiating between valid traffic and the attacker's packets. The main challenge in presenting such a solution is to exploit existing packet-filtering mechanisms in a way that allows fast processing of packets but is complex enough so that the attacker cannot efficiently craft packets that pass the filters. We show a protocol that mitigates DoS attacks by adversaries that can eavesdrop and (with some delay) adapt their attacks accordingly. The protocol uses only available efficient packet-filtering mechanisms based mainly on addresses and port numbers. Our protocol avoids the use of fixed ports and instead performs "pseudorandom port hopping." We model the underlying packet-filtering services and define measures for the capabilities of the adversary and for the success rate of the protocol. Using these, we provide a novel rigorous analysis of the impact of DoS on an end-to-end protocol and show that our protocol provides effective DoS prevention for realistic attack and deployment scenarios. [J585]

"Multi-Tier Cooperative Broadcasting with Hierarchical Modulations"

We consider broadcasting to multiple destinations with uneven quality receivers. Based on their quality of reception, we group destinations in tiers and transmit using hierarchical modulations. These modulations are known to offer a practical means of achieving variable error protection of the broadcasted information to receivers of variable quality. After the initial broadcasting step, tiers successively re-broadcast part of the information they received from tiers of higher-quality to tiers with lower reception capabilities. This multi-tier cooperative broadcasting strategy can accommodate variable rate and error performance for different tiers but requires complex demodulation steps. To cope with this complexity in demodulation, we derive simplified per-tier detection schemes with performance close to maximum-likelihood and ability to collect the diversity provided as symbols propagate through diversified channels across successive broadcastings. Error performance is analyzed and compared to (non)-cooperative broadcasting strategies. Simulations corroborate our theoretical findings. [J586]

"A Fine-Grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks"

Distributed peer-to-peer (P2P) applications have been gaining momentum recently. In such applications, all participants are equal peers simultaneously functioning as both clients and servers to each other. A fundamental problem is, therefore, how to select reliable servers from a vast candidate pool. To answer this important open question, we present a novel reputation system built upon the multivariate Bayesian inference theory. Our system offers a theoretically sound basis for clients to predict the reliability of candidate servers based on self-experiences and feedbacks from peers. In our system, a fine-grained quality of service (QoS) differentiation method is designed to satisfy the diverse QoS needs of individual nodes. Our reputation system is also application-independent and can simultaneously serve unlimited P2P applications of different type. Moreover, it is semidistributed in the sense that all application-related QoS information is stored across system users either in a random fashion or through a distributed hash table (DHT). In addition, we propose to leverage credits and social awareness as reliable means of seeking honest feedbacks. Furthermore, our reputation system well protects the privacy of users offering feedbacks and is secure against various attacks such as defaming, flattering, and the Sybil attack. We confirm the effectiveness and efficiency of the proposed system by extensive simulation results. [J587]

"Encryption: Security Considerations for Portable Media Devices"

With the proliferation of removable media devices, such as iPods and USB drives, large amounts of an organization's sensitive data can easily be removed. The author explores the complexities of protecting networks against removable media, including guidelines for purchasing encryption software. This article examines how to develop portable and removable media security policies, as well as how encryption can assist in authenticating, authorizing, and auditing removable media devices. [J588]

"Data Sharing across the Atlantic"

Government tend to be reluctant to submit their policies to democratic oversight, but in the US the Congress and the judiciary ultimately can and will hold the administration to account. Due to its constitutional peculiarities, however, Europe lacks adequate mechanisms for scrutinizing EU law enforcement and security policies: there's neither a European federal executive to hold accountable nor any way to hold the 27 member states' national governments to count for EU "federal" policies. Collecting each category of personal data might not individually constitute unacceptable violation at our privacy; but the cumulated measures of data collection and other observation mechanisms lead to a near complete surveillance of all citizens [J589]

"Reversible Data-Hiding Scheme for 2-D Vector Maps Based on Difference Expansion"

Reversible watermarking is suitable for hiding data in 2-D vector maps because the distortions induced by data embedding can be removed after extracting the hidden bits. In this paper, two reversible data-hiding schemes are explored based on the idea of difference expansion. The first scheme takes the coordinates of vertices as the cover data and hides data by modifying the differences between the adjacent coordinates. The scheme achieves high capacity in the maps with highly correlated coordinates. Instead of the raw coordinates, the second scheme adopts the manhattan distances between neighbor vertices as the cover data. A set of invertible integer mappings is defined to extract manhattan distances from coordinates and the hidden data are embedded by modifying the differences between the adjacent distances. For those maps where distances exhibit high correlation, this scheme shows better performance than the former one, both in capacity and invisibility. Three different maps with distinct features are used for the experiments. The results indicate that two proposed schemes suit different types of maps, respectively, according to the correlation of the selected cover data. Both schemes are strictly reversible. In addition, they can be slightly robust for low amplitude distortions by selecting higher digits for data hiding. The potential applications of proposed schemes may include map data authentication, secret communication, etc. [J590]

"Double-Sided Watermark Embedding and Detection"

Spread-spectrum schemes embed additive or multiplicative watermarks into the host contents for copyright protection. However, their performances are reduced by the interference from the host contents. Thus, in this work, we introduce a simple double-sided technique to utilize this interference for performance improvements. Different from the previous host interference rejection schemes, it does not reject the host interference. However, it can also achieve great performance enhancement over the traditional spread-spectrum schemes. Moreover, due to this nice property of not rejecting the host interference, it has a big advantage over the host interference rejection schemes in that the perceptual analysis can be easily implemented for our scheme to improve the perceptual quality of the watermarked contents. Our technique is effectively employed in both additive and multiplicative spread-spectrum schemes. Finally, its performance advantage is demonstrated through both theoretical and empirical comparisons. [J591]

"Protecting Biometric Templates With Sketch: Theory and Practice"

Secure storage of biometric templates has become an increasingly important issue in biometric authentication systems. We study how secure sketch, a recently proposed error-tolerant cryptographic primitive, can be applied to protect the templates. We identify several practical issues that are not addressed in the existing theoretical framework, and show the subtleties in evaluating the security of practical systems. We propose a general framework to design and analyze a secure sketch for biometric templates, and give a concrete construction for face biometrics as an example. We show that theoretical bounds have their limitations in practical schemes, and the exact security of the system often needs more careful investigations. We further discuss how to use secure sketch in the design of multifactor authentication systems that allow easy revocation of user credentials. [J592]

"Guest Editorial: Special Issue on Human Detection and Recognition"

The 12 regular papers and three correspondences in this special issue focus on human detection and recognition. The papers represent gait, face (3-D, 2-D, video), iris, palmprint, cardiac sounds, and vulnerability of biometrics and protection against the spoof attacks. [J593]

"Watermarking Protocol for Web Context"

Digital watermarking is considered to be a main technology for the copyright protection of multimedia digital content distributed on the Internet. However, watermarking procedures can effectively support copyright protection processes only if they are applied by employing specific watermarking protocols, which define the scheme of the interactions that have to take place among the entities involved in the content protection and web-based distribution. To this end, a number of current watermarking protocols can attain important achievements, such as the correct authentication of buyers without exposing their identities during web transactions and the capability of resorting to trusted watermark certification authorities to ensure a copyright protection process that is able to correctly take into account the rights of both buyers and sellers. However, these protocols are often not suitable for web context, where buyers are usually neither provided with digital certificates issued by trusted certification authorities nor able to autonomously perform complex security actions to purchase digital content distributed by web-based content providers. This paper presents an improved version of a web-oriented and interactive anonymous buyer-seller watermarking protocol previously presented by the author. The protocol overcomes the drawbacks affecting relevant protocols existing in literature, and is based on a design approach that makes it suitable for web contexts. [J594]

"Distributed Source Coding for Multimedia Multicast Over Heterogeneous Networks"

Real-time multimedia multicast over wireless networks is an exciting application that has generated a lot of interest recently. Its main challenge lies in the stringent bandwidth and time-delay requirements of real-time multimedia and severe impairments of the wireless channels. We develop a network-aware cross-layer design for multimedia multicast over heterogeneous wireless-wireline networks, that leverages the knowledge on network information theory, multimedia processing, error control, and networking. In particular, the encoded multimedia data are broadcast to multiple Internet servers over a wireless radio link. Each server merely compresses the signal it has received using distributed source coding by exploiting mutual correlation among signals received at different servers. The receiver collects bitstreams from the servers before performing joint decoding. We provide an algorithm for optimal nonuniform scalar quantizer design at the server side that minimizes the required rate under the decoder bit error rate constraint. For scalable multimedia codes, we develop a joint source-channel coding scheme which combines error-protection at the base station and distributed source coding at the servers. Our experimental results show significant performance improvements over conventional solutions due to spatial diversity and distributed source coding gains. [J595]

"Data Mining Approach to Threshold Settings of Islanding Relays in Distributed Generation"

This paper introduces a new approach for determination of the threshold settings of islanding relays in distributed generation (DG) interconnections. This approach uses data-mining technology to extract the optimal relay settings information from a large data set of system parameters. This data is constructed from offline simulation analyses of events and consequences. The mining of these consequences defines the boundary limits of the threshold settings that could secure the detection of islanding operations under: minimum detectable zones, multiple distributed resources (DRs), diverse distributed resource technologies, various operating conditions, and different network topologies. The approach is tested on a typical DG with multiple distributed resources, and the results indicate that this approach can be used effectively to support the setting relay decision. [J596]

"Cooperative Source and Channel Coding for Wireless Multimedia Communications"

Past work on cooperative communications has indicated substantial improvements in channel reliability through cooperative transmission strategies. To exploit cooperation benefits for multimedia transmission over slow fading channels, we propose to jointly allocate bits among source coding, channel coding and cooperation to minimize the expected distortion of the reconstructed signal at the receiver. Recognizing that, not all source bits are equally important in terms of the end-to-end distortion, we further propose to protect the more important bits through user cooperation. We compare four modes of transmission that differ in their compression and error protection strategies (single layer or multiple layer source coding with unequal error protection, with versus without cooperation). Our study includes an i.i.d. Gaussian source as well as a video source employing an H.263+ codec. We present an information theoretic analysis for the Gaussian source to investigate the effects of the modulation scheme, bandwidth ratio (number of channel uses per source sample), and average link signal-to-noise ratios on the end-to-end distortion of the four modes studied. The information theoretic observations are validated using practical channel coding simulations. Our study for video considers error propagation in decoded video due to temporal prediction and jointly optimizes a source coding parameter that controls error propagation, in addition to bits for source coding, channel coding and cooperation. The results show that cooperation can significantly reduce the expected end-to-end distortion for both types of source and that layered cooperation provides further improvements and extends the benefits to a wider range of channel qualities. [J597]

"An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics"

Polygonal lines constitute a key graphical primitive in 2D vector graphics data. Thus, the ability to apply a digital watermark to such an entity would enable the watermarking of cartoons, drawings, and geographical information systems (GIS) data in vector graphics format. This paper builds on and extends an existing algorithm that achieves polygonal line watermarking by modifying the Fourier descriptors magnitude in an imperceptible way. Watermarks embedded by this technique can be detected in rotated, translated, scaled, or reflected polygonal lines. The detection of such watermarks had been previously carried out through a correlator detector. In this paper, analysis of the statistics of the Fourier descriptors is exploited to devise an optimal blind detector. Furthermore, the problem of watermarking multiple lines, as well as other implementation issues are being addressed. Experimental results verify the imperceptibility and robustness of the proposed method. [J598]

"Improving the Error Rate Performance of Turbo Codes using the Forced Symbol Method"

This letter presents a method that significantly improves the error rate performance of turbo codes, especially in the error flare region, without changing the basic encoder structure. This method applies repeated decoding, with

one or more symbols being forced to certain values, when an error is detected. This forces the decoder to output alternate sets of decisions that can then be checked for errors. The effectiveness of this method is demonstrated by its ability to lower the error flare by several orders of magnitude as soon as the error flare region is encountered. For the DVB-RCS 8-state, rate 1/2, double-binary turbo code and packets of 1504 information bits (MPEG-size), this method yields performance about 0.4 dB from the sphere-packing bound down to a packet error rate of 10-7. [J599]

"News Briefs"

This paper briefly describes (1) security, including network security, malware, cyberware etc., (2) privacy, including transportation security administration, data sharing agreement etc., and (3) policy, including spy act, government approved legislation etc. [J600]

"MEMS-Assisted Cryptography for CPI Protection"

The authors present a concept for an anti-tamper system that dynamically generates a cryptographic key derived from microelectromechanical systems (MEMS) arrays encapsulated within a protected system in a single package. The system provides protection in active and passive states with no battery backup. [J601]

"AnySpot: Pervasive Document Access and Sharing"

The World Wide Web, wireless devices, and wireless networks have increased the opportunities for supporting pervasive document access and sharing. However, today's solutions remain spotty in their coverage for pervasive information needs. To address this, AynSpot is developed, a Web-service-based platform that seamlessly connects users to personal and shared documents wherever they go, meeting several key requirements of pervasive information access. This paper describes AnySpot's design principles and report our experience deploying it in a large, multinational organization. [J602]

"Ultrafast Potential-Backup-Cost (PBC)-Based Shared Path Protection Schemes"

This paper describes a novel ultrafast heuristic algorithm to address an NP-hard optimization problem. One of the significant and nonintuitive results is that the schemes based on the heuristic can achieve a better overall performance than their time-consuming integer-linear-programming-based counterparts. More specifically, the proposed schemes are useful in providing an online shared path protection by establishing survivable connections in high-speed networks. The advantage of our heuristic algorithm over the existing heuristic algorithms in finding a pair of link-disjoint paths, which are called active and backup paths, comes from the following salient feature. It uses a so-called potential-backup-cost (PBC) function when selecting an active path in the first phase to take into consideration the backup bandwidth needed by the corresponding backup path, which has yet to be chosen in the second phase. The PBC function is derived mathematically based on the statistical analysis of experimental data. While the use of PBC only requires partial aggregate information on how the existing connections are established in a network, it can also be applied even more effectively when complete information is available. [J603]

"Unequal error protection for LZSS compressed data using Reed-Solomon codes"

An unequal error protection strategy for minimising the impact of error bursts in the storage or transmission of compressed data has been proposed. The strategy is designed for the LZSS algorithm, which is a dynamic dictionary compression method. Through extensive computer simulations we investigate which information classes within LZSS are more sensitive to burst errors. Based on these results, an unequal error protection strategy that greatly reduces the error propagation during the decompression process has been proposed. Numerical results using text files from a common database are presented. [J604]

"Selective Protection Analysis Using a SEU Emulator: Testing Protocol and Case Study Over the Leon2 Processor"

VLSI circuits for space application must be protected by the insertion of massive redundancy. However, this increases silicon area and the production costs, therefore designers can often consider leaving some large, noncritical subcircuits unprotected. This paper presents how FT-UNSHADES, a nonintrusive tool for fault injection on emulated hardware, helps designers to select the proper level of protection in every subcircuit. Using FT-UNSHADES, a test procedure is proposed that provides: 1) information about the quality of the test vectors, 2) a proper estimation of the number of injected faults required to get confidence about the results of a fault injection campaign, and 3) information about the criticality of individual subcircuits by selective fault injection campaigns. In addition, FT-UNSHADES allows the insertion of multi-bit flips. This test procedure has been

applied to three different, protected and unprotected, versions of the well-known Leon2 processor, and the results are discussed here. [J605]

"Beyond Secrecy: New Privacy Protection Strategies for Open Information Spaces"

When the US government erected export-control barriers against the cryptographic technology used to ensure data confidentiality, a coalition of privacy advocates joined IT companies to get those barriers removed and enable widespread adoption of encryption for privacy protection. The most fundamental challenge to 20th century privacy laws is more social than technical-adding to the stream of personal data is a new wave of user-generated content in the form of blogs. Access control and security techniques will remain vital to privacy protection-access control is important for protecting sensitive information and, above all, preserving anonymity. [J606]

"Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels"

Capability of accurately locating tampered pixels is desirable in image authentication. We propose a novel statistical scheme of fragile watermarking, in which a set of tailor-made authentication data for each pixel together with some additional test data are embedded into the host image. On the authentication side, examining the pixels and their corresponding authentication data will reveal the exact pattern of the content modification. As long as the tampered area is not too extensive, two distinct probability distributions corresponding to tampered and original pixels can be used to exactly identify the tampered pixels. [J607]

"Informationally Decentralized Video Streaming Over Multihop Wireless Networks"

Various packet scheduling, dynamic routing, error-protection, and channel adaptation strategies have been proposed at different layers of the protocol stack to address multi-user video streaming over multihop wireless networks. However, these cross-layer transmission strategies can be efficiently optimized only if they use accurate information about the network conditions and hence, are able to timely adapt to network changes. Due to the informationally decentralized nature of the multihop wireless network, performing centralized optimization for delay-sensitive video streaming application based on global information about the network status is not practical. Distributed solutions that adapt the transmission strategies based on timely information feedback need to be considered. To acquire this information feedback for cross-layer adaptation, we deploy an overlay infrastructure, which is able to relay the necessary information about the network status and incurred delays across different network ldquohorizonsrdquo (i.e., across a different number of hops in a predetermined period of time). In this paper, we propose a distributed streaming approach that is optimized based on the local information feedback acquired from the various network horizons. We investigate the distributed cross-layer adaptation at each wireless node by considering the advantages resulting from an accurate and frequent network information feedback from larger horizons as well as the drawbacks resulting from an increased transmission overhead. Based on the information feedback, we can estimate the risk that packets from different priority classes will not arrive at their destination before their decoding deadline expires. Subsequently, the various transmission strategies such as packet scheduling, retransmission limit and dynamic routing policies are adapted to jointly consider the estimated risk as well as the impact in terms of distortion of the different priority classes. Our results show that--the proposed dynamic routing policy based on timely information feedback outperforms existing state-of-the-art on-demand routing solutions by more than 2 dB in terms of the received video quality. [J608]

"Scalable H.264/AVC Video Transmission Over MIMO Wireless Systems With Adaptive Channel Selection Based on Partial Channel Information"

In this paper, we present a novel joint application physical-layer design (JAPLD) strategy to cost-effectively transmit scalable H.264/AVC video over multi-input multi-output (MIMO) wireless systems. With this approach, the application layer cooperates with the physical layer to maximize the system performance. First, in physical layer, we propose a new layered video transmission scheme over MIMO: adaptive channel selection (ACS). ACS-MIMO is fundamentally different from parallel transmission MIMO (PT-MIMO). While each bit stream is continuously transmitted through a fixed antenna in PT-MIMO, ACS-MIMO is able to periodically switch each bit stream among multiple antennas. In application layer, Scalable Video Coding (SVC) generates layered bit streams that need prioritized delivery. Then, we obtain the ordering of each subchannel's SNR strength as partial channel information (CI) at the receiver. The partial CI is acquired via the estimated channel state information based on training sequences. The JAPLD strategy we developed in this research shall switch the bit stream automatically to match the ordering of SNR strength for the subchannels. Essentially, we will launch higher priority layer bit stream into higher SNR strength subchannel by the proposed JAPLD algorithm. In this fashion, we can implicitly achieve automatic unequal error protection (UEP) for layered SVC transmission over MIMO

system without power control at the transmitter. Experimental results show that the proposed ACS-MIMO system is able to achieve UEP with the obtained partial CI and the reconstructed video peak signal-to-noise ratio demonstrate the performance improvement of the proposed system as compared with open loop PT-MIMO system. [J609]

"Handling Multiple Credentials in a Heterogeneous SOA Environment"

With all the diverse technology in a typical corporate IT environment, it's no surprise that multiple types and formats of security credentials exist, each one designed to protect its respective software system. We can address the problem of handling multiple credential types and formats in a heterogeneous SOA environment by using a data structure designed not only to store and propagate user credential information but also to accurately reflect trust relationships between credential instances. Modeling credentials in this manner leads to improved assurance for applications that need to enforce security policies, either based on business rules established at the corporate level or by compliance to the relevant security specifications. [J610]

"Balancing Privacy and Risk in the E-Messaging World"

Messaging within an enterprise used to be like the local water department; as long as the email flowed, no one paid any attention to it and all was good. Things are different now-messaging has become the center of a legal and regulatory maelstrom. It's the confluence of security, privacy, and opportunity within an organization. Email and instant messaging reduce the cost of delivering products, increase responsiveness to customers, enfranchise distance expertise, and evenly balance employee work/home responsibilities. Yet, these very same technologies open the door to intellectual property loss, malware intrusions, employee harassment, and compliance violations. [J611]

"Trust on a Nationwide Scale"

Singapore is a small island nation with roughly 4.5 million inhabitants, but it has a highly developed international economy based on trade, services, and knowledge management. Singapore launched its lofty goals by defining the nationpsilas e-security. Current research in the Singaporean telecommunications and IT security community attempts to model such peer-to-peer ad hoc transactions and leverage the existing standard infrastructure described in this article. [J612]

"The Design and Performance of Distributed LT Codes"

This paper describes techniques to decompose LT codes (a class of rateless erasure-correcting codes) into distributed LT (DLT) codes. DLT codes can be used to independently encode data from multiple sources in a network in such a way that, when the DLT-encoded packets are combined at a common relay, the resulting bit stream (called a modified LT (MLT) code) has a degree distribution approximating that of an LT code, with simulations indicating comparable performance. In essence, DLT codes are designed so that the final stage of encoding for erasure correction can be carried out by a low-complexity relay that selectively xors the bit streams generated at each source and transmits the result to the sink. This paper presents results for two-source and four-source networks. It is shown that, when the relay-to-sink link is the bottleneck, the DLT/MLT approach can yield substantial performance benefits compared with a competing strategy wherein each of the sources uses its own independent LT encoder and the resulting bit streams are time-multiplexed through the relay. [J613]

"The Canadian Response to the USA Patriot Act"

The border between Canada and the US is often hailed as the longest undefended border in the world. This is true for the physical border, dotted with sporadic land crossings, and even more so for the digital border, where thousands of strands of fiber span the frontier without any regulation or formality. Since the attacks of September 11, 2001, US authorities have spent untold millions of dollars guarding their frontiers to regulate what gets into the country. On the other side of the border, many Canadian jurisdictions have turned their thoughts to regulating what information flows southward, into the US. This isn't out of concern about terrorism but rather about the US response to terrorism. [J614]

"Visual Discovery in Computer Network Defense"

Computer network defense (CND) requires analysts to detect both known and novel forms of attacks in massive volumes of network data. It's through discovering the unexpected that CND analysts detect new versions of mal ware (such as viruses and Trojan horses) that have passed through their antivirus products, new methods of intrusion that have breached their firewalls and intrusion detection systems (IDSs), and new groups of cyber-criminals pressing the attack. This paper presents visual assistant for information assurance analysis. VIAssist is

a visualization framework based on a comprehensive cognitive task analysis of CND analysts, and so fits their work practices and operational environment. [J615]

"Advanced Conditional Access System for Digital Broadcasting Receivers Using Metadata"

This paper presents an advanced conditional access system (CAS) for digital broadcasting receivers using program-related information called metadata. Digital broadcasting receivers using metadata (DBRM) provide services enhanced by using metadata and content stored in receivers, but it is so easy to edit stored content by using metadata that broadcasters require a content usage control mechanism for DBRM. The advanced CAS provides a secure environment for content and metadata in digital broadcasting receivers by preventing tampering and ensuring that only metadata certified by the broadcaster can be used. To evaluate the advanced CAS, we also developed a smart card and a prototype receiver on a PC. We have demonstrated in an implementation experiment that the advanced CAS can be implemented securely and utilized in broadcasting services using DBRM. [J616]

"Hydraulic Splines: A Hybrid Approach to Modeling River Channel Geometries"

The hydraulic spline algorithm generates irregular 2D channel grids from highly accurate cross-sectional survey data at any desired resolution, facilitating its integration with high-density light detection and ranging (lidar) data. [J617]

"Managing Enterprise Security Risk with NIST Standards"

Federal agencies and private-sector organizations are increasingly concerned with the risks that today's sophisticated cyberthreats pose to critical enterprise missions and business functions. Federal Information Security Management Act (FISMA) established sweeping information security (IS) requirements for the federal government and contractors, and it made the National Institute of Standards and Technology (NIST) responsible for developing IS standards and guidelines to allow for compliance. NIST faced the challenging task of establishing mandatory minimum IS standards and guidelines for the federal government and supporting contractors, while ensuring flexible implementation based on diverse missions and business functions. [J618]

"A Review of Network Security"

A review of Introduction to Network Security by Neal Krawetz [J619]

"Cyclic Algebras for Noncoherent Differential Space-Time Coding"

We investigate cyclic algebras for coding over the differential noncoherent channel. Cyclic algebras are an algebraic object that became popular for coherent space-time coding, since it naturally yields linear families of matrices with full diversity. Coding for the differential noncoherent channel has a similar flavor in the sense that it asks for matrices that achieve full diversity, except that these matrices furthermore have to be unitary. In this work, we give a systematic way to find infinitely many unitary matrices inside cyclic algebras, which holds for all dimensions. We show how cyclic algebras generalize previous families of unitary matrices obtained using the representation of fixed-point-free groups. As an application of our technique, we present families of codes for three and four antennas that achieve high coding gain. [J620]

"Devising Post-Disaster Continuity Plans that Meet Actual Recovery Needs"

This article is based on the author's direct observation, participation, and field experience in more than fifteen hundred post disaster recoveries over the last fifteen years. A review of relevant literature is followed by a discussion of the social dynamics of organizations recovering from a disaster; including the inventory period that immediately follows a disaster, three group defensive systems that emerge to defend the group against the threat and why one of these performs significantly better than the others. This is followed by a brief post-disaster timeline indicating the timing of crisis where staff morale becomes a critical issue and when political realignments become necessary. Lastly, conditions for selection and membership on a business resilience/recovery team and advantages of building this process into normal business practices are discussed. [J621]

"A System for the Measurement of the Amazon"

The System for the Vigilance of the Amazon (SIVAM) is a $1.4 billion dollar project of Brazil aimed at the development and deployment of a high-technology system-of-systems to perform monitoring, protection, and control of the land, air, and water resources of the Brazilian Amazon region. The primary challenge of the SIVAM project is to perform remote sensing and communications over a vast and undeveloped land area. The SIVAM

network meets this challenge through an extensive network of Air Traffic Control/Surveillance Radars, Environmental Sensors, Communications Systems, Airborne Sensor Systems, and Coordination Centers. Now fully operational, the SIVAM system is the world's largest fully integrated remote monitoring system of the environment and provides critical information on a timely basis to the Brazilian government, law enforcement agencies, and to commercial, educational, and research groups. [J622]

"How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum"

In this article, we provide a brief history of the Cyber Defense Exercise (CDX), describe Air Force Institute of Technology (AFIT's) participation in it, and explain how the experience shaped the information-assurance curriculum and course format at AFIT. The CDX is an annual competition designed to give students the opportunity to learn and demonstrate best practices in defensive information assurance. The CDX's fundamental objective is to design and implement a network that provides specified IT services and defend it against an onslaught of cyberattacks and natural events. CDX participants included blue forces (students), red forces (attacker) and a white cell. [J623]

"Computation of Transient Overvoltages in Low-Voltage Installations During Direct Strikes to Different Lightning Protection Systems"

This paper presents a numerical electromagnetic analysis of loop-termination voltages inside an outer lightning protection system (LPS) resulting from direct lightning strikes. The method of moments is combined with the transmission line model, and employed to model the whole structure in three dimensions and the lightning channel, respectively. Three distinct standard LPS classes and a nonstandard LPS are modeled, namely, LPS1, LPS2, and LPS4, and LPS0, respectively. All cases are simulated using the negative subsequent stroke current at lightning protection level II according to IEC 62305-1. Three distinct current waveforms are selected in order to simulate the variety of different current rises. Three single-phase parallel vertical loops are simulated inside the struck LPS. The results reveal that reducing the LPS mesh width improves its shielding performance, where this may be a basic method to damp the lightning-induced voltages with little dependency on the strike location, and without any appreciable effect of the LPS material. The variation of the lightning-current front shows that the loop-termination voltages are altered within a factor of about 2. Existence and interconnection of extra protective earthing, e.g., via information technology cables, and the value and type of the loop-termination impedance also have significant influence on such voltages. [J624]

"Trust-based privacy preservation for peer-to-peer data sharing"

Privacy preservation in a peer-to-peer (P2P) system tries to hide the association between the identity of a participant and the data that it is interested in. This paper proposes a trust-based privacy-preservation method for P2P data sharing. It adopts the trust relation between a peer and its collaborators (buddies). The buddy works as a proxy to send the request and acquire the data. This provides a shield under which the identity of the requester and the accessed data cannot be linked. A privacy measuring method is presented to evaluate the proposed mechanism. Dynamic trust assessment and the enhancement to supplier's privacy are discussed [J625]

"The Boneh-Shaw fingerprinting scheme is better than we thought"

Digital fingerprinting is a forensic method against illegal copying. The distributor marks each individual copy with a unique fingerprint. If an illegal copy appears, it can be traced back to one or more guilty pirates due to this fingerprint. To work against a coalition of several pirates, the fingerprinting scheme must be based on a collusion-secure code. This paper addresses binary collusion-secure codes in the setting of Boneh and Shaw (1995/1998). We prove that the Boneh-Shaw scheme is more efficient than originally proven, and we propose adaptations to further improve the scheme. We also point out some differences between our model and others in the literature. [J626]

"Efficient spatial image watermarking via new perceptual masking and blind detection schemes"

The aim of this paper is to improve the performance of spatial domain watermarking. To this end, a new perceptual mask and a new detection scheme are proposed. The proposed spatial perceptual mask is based on the cover image prediction error sequence and matches very well with the properties of the human visual system. It exhibits superior performance compared to existing spatial masking schemes. Moreover, it allows for a significantly increased strength of the watermark while, at the same time, the watermark visibility is decreased. The new blind detection scheme comprises an efficient prewhitening process and a correlation-based detector. The prewhitening process is based on the least-squares prediction error filter and substantially improves the detector's performance. The correlation-based detector that was selected is shown to be the most suitable for

the problem at hand. The improved performance of the proposed detection scheme has been justified theoretically for the case of linear filtering plus noise attack and through extensive simulations. The theoretical analysis is independent of the proposed mask and the derived expressions can be used for any watermarking technique based on spatial masking. It is shown though that in most cases the detector performs better if the proposed mask is employed. [J627]

"Steganalysis for Markov cover data with applications to images"

The difficult task of steganalysis, or the detection of the presence of hidden data, can be greatly aided by exploiting the correlations inherent in typical host or cover signals. In particular, several effective image steganalysis techniques are based on the strong interpixel dependencies exhibited by natural images. Thus, existing theoretical benchmarks based on independent and identically distributed (i.i.d.) models for the cover data underestimate attainable steganalysis performance and, hence, overestimate the security of the steganography technique used for hiding the data. In this paper, we investigate detection-theoretic performance benchmarks for steganalysis when the cover data are modeled as a Markov chain. The main application explored here is steganalysis of data hidden in images. While the Markov chain model does not completely capture the spatial dependencies, it provides an analytically tractable framework whose predictions are consistent with the performance of practical steganalysis algorithms that account for spatial dependencies. Numerical results are provided for image steganalysis of spread-spectrum and perturbed quantization data hiding. [J628]

"A scheme for privacy-preserving data dissemination"

An adequate level of trust must be established between prospective partners before an interaction can begin. In asymmetric trust relationships, one of the interacting partners is stronger. The weaker partner can gain a higher level of trust by disclosing private information. Dissemination of sensitive data owned by the weaker partner starts at this moment. The stronger partner can propagate data to others, who may then choose to spread data further. The proposed scheme for privacy-preserving data dissemination enables control of data by their owner (such as a weaker partner). It relies on the ideas of bundling sensitive data with metadata, an apoptosis of endangered bundles, and an adaptive evaporation of bundles in suspect environments. Possible applications include interactions among patients and healthcare providers, customers and businesses, researchers, and suppliers of their raw data. They will contribute to providing privacy guarantees, which are indispensable for the realization of the promise of pervasive computing [J629]

"Joint coding and embedding techniques for MultimediaFingerprinting"

Digital fingerprinting protects multimedia content from illegal redistribution by uniquely marking every copy of the content distributed to each user. The collusion attack is a powerful attack where several different fingerprinted copies of the same content are combined together to attenuate or even remove the fingerprints. One major category of collusion-resistant fingerprinting employs an explicit step of coding. Most existing works on coded fingerprinting mainly focus on the code-level issues and treat the embedding issues through abstract assumptions without examining the overall performance. In this paper, we jointly consider the coding and embedding issues for coded fingerprinting systems and examine their performance in terms of collusion resistance, detection computational complexity, and distribution efficiency. Our studies show that coded fingerprinting has efficient detection but rather low collusion resistance. Taking advantage of joint coding and embedding, we propose a permuted subsegment embedding technique and a group-based joint coding and embedding technique to improve the collusion resistance of coded fingerprinting while maintaining its efficient detection. Experimental results show that the number of colluders that the proposed methods can resist is more than three times as many as that of the conventional coded fingerprinting approaches. [J630]

"A warning to industry-fix it or lose it"

As part of its security analysis and the Industry Trends series, Morgan Stanley has identified the endpoint as critical for winning the security war rather than just fighting hapless battles. For the Internet to be a truly reliable and trusted commerce mechanism, protecting a transaction's source is imperative. Other than protecting the data itself, endpoint integrity is at this point the most critical element in getting back on track [J631]

"Fault evaluation for security-critical communication devices"

Communications devices for government or military applications must keep data secure, even when their electronic components fail. Combining information flow and risk analyses could make fault-mode evaluations for such devices more efficient and cost-effective. Conducting high-grade information security evaluations for computer communications devices is intellectually challenging, time-consuming, costly, and error prone. We believe that our structured approach can reveal potential fault modes because it simplifies evaluating a device's

logical design and physical construction. By combining information-flow and risk-analysis techniques, evaluators can use the process to produce a thorough and transparent security argument. In other work, we have applied static analysis techniques to the evaluation problem, treating a device's schematic circuitry diagram as an information flow graph. This work shows how to trace information flow in different operating modes by representing connectivity between components as being conditional on specific device states. We have also developed a way to define the security-critical region of components with particular security significance by identifying components that lie on a path from a high-security data source to a low-security sink. Finally, to make these concepts practical, we have implemented them in an interactive analysis tool that reads schematic diagrams written in the very high speed integrated circuit (VHSIC) hardware description language. [J632]

"PacketScore: a statistics-based packet filtering scheme against distributed denial-of-service attacks"

Distributed denial-of-service (DDoS) attacks are a critical threat to the Internet. This paper introduces a DDoS defense scheme that supports automated online attack characterizations and accurate attack packet discarding based on statistical processing. The key idea is to prioritize a packet based on a score which estimates its legitimacy given the attribute values it carries. Once the score of a packet is computed, this scheme performs score-based selective packet discarding where the dropping threshold is dynamically adjusted based on the score distribution of recent incoming packets and the current level of system overload. This paper describes the design and evaluation of automated attack characterizations, selective packet discarding, and an overload control process. Special considerations are made to ensure that the scheme is amenable to high-speed hardware implementation through scorebook generation and pipeline processing. A simulation study indicates that packetscore is very effective in blocking several different attack types under many different conditions [J633]

"Mobile technology as a learning object and an exploration tool in an IS curriculum: an innovative instruction of wireless network security"

Information systems (IS) is a fully recognized business discipline. Many IS programs have not given network security appropriate attention; nor have they brought enough hands-on experience of both wireline and wireless networks to the class rooms. This study proposes a systematic framework to cover wireless security attack, detection, and protection. It also includes a learning matrix for educators and practitioners to enhance the IS curriculum. The assessment results show that students are very positive toward this new approach of security education. Implications and suggestions are provided [J634]

"Randomness in cryptography"

Although more formal definitions of randomness exist, a colloquial one will suffice here: a random process is one whose consequences are unknown. Intuitively, this is why randomness is crucial in cryptographic applications-because it provides a way to create information that an adversary can't learn or predict. It's then the task of a good protocol designer to leverage this power in the best possible way to protect data and communication. In this paper, we'll look at some basic uses of randomness in cryptography and briefly review the process of securely generating randomness [J635]

"Applying multi-agent system technology in practice: automated management and analysis of SCADA and digital fault recorder data"

This paper reports on the use of multi-agent system technology to automate the management and analysis of SCADA and digital fault recorder (DFR) data. The multi-agent system, entitled Protection Engineering Diagnostic Agents (PEDA), integrates legacy intelligent systems that analyze SCADA and DFR data to provide data management and online diagnostic information to protection engineers. Since November 2004, PEDA agents have been intelligently interpreting and managing data online at a transmission system operator in the U.K. As the results presented in this paper demonstrate, PEDA supports protection engineers by providing access to interpreted power systems data via the corporate intranet within minutes of the data being received. In this paper, the authors discuss their experience of developing a multi-agent system that is robust enough for continual online use within the power industry. The use of existing agent development toolsets and standards is also discussed. [J636]

"Nonlinear collusion attack on a watermarking scheme for buyer authentication"

This paper presents an adaptive collusion attack on a buyer authentication watermarking scheme. To accomplish this attack, the traitors (i.e., dishonest buyers) select the pixels of their watermarked images generated from the same original image and average the selected pixels so as to remove the watermark information. Additionally,

the forged image is of higher quality than any watermarked image. Both theoretical and experimental results demonstrate that our attack is very effective. [J637]

"Secure electronic markets for private information"

Technological advances in the collection, storage, and analysis of data have increased the ease with which businesses can make profitable use of information about individuals. Some of this information is private, and individuals are simultaneously becoming more aware of the value of the information and how the loss of control over this information impacts their personal privacy. As a partial solution to these concerns, this paper presents a mechanism that serves two purposes. The first enables the use of private, numerical data in the answering of queries while simultaneously providing a security feature that protects the data owners from a loss of privacy that could result from an unauthorized access. The second develops a compensation model for the use of the data that allows individuals to dynamically redefine their security requirements. The compensation model is built on the information-security mechanism to create the foundation of a market for private information. This paper illustrates how compensation models like the one presented here could be used in a self-regulating market for private information. Additionally, the compensation component of an intermediated market for private information is developed and extensively analyzed. Finally, this paper provides insights and draws several important conclusions on markets for private information [J638]

"Autonomic-computing approach to secure knowledge management: a game-theoretic analysis"

The explosion of knowledge management systems (KMS) and the need for their wide accessibility and availability has created an urgent need for reassessing the security practices and policies in organizations. Security of these assets is a day-to-day job placing a tremendous cognitive load on information-technology (IT) professionals, which can make it almost impossible to manage the security aspects of KMS. Autonomic-computing systems are well suited to manage KMS, as they use high-level system objectives provided by administrators as the basis for managing the security of KMS. The authors model the self-protection and self-healing configuration attributes in autonomic systems through game-theoretic models. The proposed modeling approach progressively moves from a manual intervention-oriented security setup to an autonomic security setup. This allows the authors to compare and contrast the different approaches and provide insights on their applicability to different security environments. The authors find that moving to a partial autonomic system with self-healing mechanisms can provide a stable environment for securing enterprise knowledge assets and can reduce hacking. It is beneficial to implement an autonomic system when manual investigation costs are higher and/or when the volume of malicious traffic is very low. An autonomic approach is especially attractive when it is difficult to impose penalties on malicious users. Autonomic systems can be effective in securing organizational knowledge assets and in reducing the potential damage from malicious users [J639]

"Secure knowledge management: confidentiality, trust, and privacy"

Knowledge management enhances the value of a corporation by identifying the assets and expertise as well as efficiently managing the resources. Security for knowledge management is critical as organizations have to protect their intellectual assets. Therefore, only authorized individuals must be permitted to execute various operations and functions in an organization. In this paper, secure knowledge management will be discussed, focusing on confidentiality, trust, and privacy. In particular, certain access-control techniques will be investigated, and trust management as well as privacy control for knowledge management will be explored [J640]

"Part 1: Special Issue on Secure Knowledge Management"

{no data available} [J641]

"Part 2: emerging issues for secure knowledge management-results of a Delphi study"

Secure Knowledge Management (SKM) is one of the emerging areas in both knowledge management and information system disciplines. SKM refers to the management of knowledge while adhering to principles of security and privacy. This study identifies key issues on SKM and draws a consensus among domain experts on the key issues. This study is an attempt to accelerate further research and development in the SKM field. In this study, the authors conducted a three-round Delphi study, identifying 21 issues in the SKM area, along with their importance and urgency ratings. Analyses show that participating experts achieved a higher level of consensus on the importance and urgency of the issue as the rounds progressed. The findings will allow both practitioners and researchers to focus and prioritize research needs in the SKM area. The paper also discusses some future-research directions [J642]

"A method for modeling marine mammal movement and behavior for environmental impact assessment"

Estimating the impact of anthropogenic sound on marine animals entails consideration of animal location in the vertical and horizontal planes and the behavior of the animal (e.g., breeding, foraging, migration) at the time of sound exposure. To approach more realistic impact estimates, the effects of sound on the marine environment (ESME) model incorporates a simulation program that permits fine-scale control over simulated marine animal (animat) movement and behavior. The simulation program, known as the Marine Mammal Movement and Behavior (3MB) module, provides user control over animats that is scaleable to available information about the species of concern. Movement and behavior is stochastically determined by sampling from distributions describing rates of movement in the horizontal and vertical planes, direction of travel, time at the surface between dives, time at depth, and time in and transition between behavioral states. Influence of behavior over each of the other distributions is permitted. As knowledge of marine animal behavior, movement, and ecology increases, the flexibility and level of control provided by such models will increase the potential for realistic impact estimates [J643]

"Digital signatures"

Many traditional and newer businesses and applications have recently been carrying out enormous amounts of electronic transactions, which have led to a critical need for protecting the information from being maliciously altered, for ensuring the authenticity, and for supporting nonrepudiation. Just as signatures facilitate validation and verification of the authenticity of paper documents, digital signatures serve the purpose of validation and authentication of electronic documents. This technology is rather new and emerging and is expected to experience growth and widespread use in the coming years. [J644]

"Reliable maps of lightning thunderstorms for Saudi Arabia"

The main objective of this research is to develop reliable maps of isokeraunic level (thunderdays/year, TD) for the country on annual and seasonal bases. New annual thunder day maps for Saudi Arabia are presented. The results in this paper are based on data and records of thunderstorm incidences in Saudi Arabia recorded by the Presidency of Metrology and Environment. These are compared with data from power system fault records and with NASA satellite data. These new maps indicate the location, frequency, and intensity of thunderstorms. Such information is useful for engineers concerned with the design and operation of transmission and distribution lines in the country, and for the more general design of lightning protection systems. Thunderstorms are most frequent in the southwest mountains in the country, reaching a maximum TD of 97; the average TD for the whole country is 26. [J645]

"Series compensated line protection enhancement by modified pilot relaying schemes"

In this paper, a comprehensive analysis of the impact of series capacitor on the performance of communication-aided distance protection schemes of transmission lines is presented. It is shown that not only the series capacitor and its overvoltage protection affect the distance protection of its line, but also the adjacent lines would experience protection problems. Mitigation of this problem is proposed by using new communication-aided schemes. The proposed schemes use the information available at the substation to inhibit relay malfunctions. The performance of the techniques is studied for different series capacitor locations in the transmission line. Real Time Digital Simulator (RTDS) and four sophisticated commercial relays are used for testing. The results verify the impact of series capacitor on the conventional communication-aided schemes and also the effectiveness of the proposed methods [J646]

"A primary and backup cooperative protection system based on wide area agents"

This paper presents a study of wide area agents based on communication for primary and backup coordinated protection. Agents are used to give each protection component control capacity as well as the ability to communicate with other agents. We feel that this method naturally points toward a new philosophy for primary and backup protection. Simulations are used to illustrate concepts, using a simulation engine called EPOCHS that combines the EMTDC/PSCAD power simulator with the NS2 network communications simulator. Results show the improved performance of our protection scheme. In this new protection system, agents were embedded in each of the conventional protection components to construct an IED relay. The agent searches for relevant information by communicating with other agents. Agent communication can take place at the same substation or at remote substations. This information can be used to detect primary and remote faults, relay misoperation, breaker failures, and to compensate such problems with a much better performance than can be done in traditional schemes. Preliminary results give us hope that the proposed protection scheme may be able to contribute toward the mitigation of wide-area disturbances and the power blackouts that frequently follow

them. [J647]

"On cosets of the generalized first-order reed-muller code with low PMEPR"

Golay sequences are well suited for use as codewords in orthogonal frequency-division multiplexing (OFDM), since their peak-to-mean envelope power ratio (PMEPR) in q-ary phase-shift keying (PSK) modulation is at most 2. It is known that a family of polyphase Golay sequences of length 2morganizes in m!/2 cosets of a q-ary generalization of the first-order Reed-Muller code, RMq(1,m). In this paper, a more general construction technique for cosets of RM q(1,m) with low PMEPR is established. These cosets contain so-called near-complementary sequences. The application of this theory is then illustrated by providing some construction examples. First, it is shown that the m!/2 cosets of RMq(1,m) comprised of Golay sequences just arise as a special case. Second, further families of cosets of RMq(1,m) with maximum PMEPR between 2 and 4 are presented, showing that some previously unexplained phenomena can now be understood within a unified framework. A lower bound on the PMEPR of cosets of RMq(1,m) is proved as well, and it is demonstrated that the upper bound on the PMEPR is tight in many cases. Finally, it is shown that all upper bounds on the PMEPR of cosets of RMq(1,m) also hold for the peak-to-average power ratio (PAPR) under the Walsh-Hadamard transform (WHT) [J648]

"Improved upper bounds for codes with unequal error protection"

Asymptotic nonexistence bounds for unequal error protecting codes with two protection levels are considered. We show that the improved estimates on the possible distance distributions for codes may sometimes yield sharper upper bounds than the previously known ones on the higher significance protection level of both nonlinear and linear codes having two protection levels. [J649]

"Contents distribution system based on MPEG-4 ISMACryp in IP set-top box environments"

DRM is a technique for preventing an illegal use of digital contents such as streaming media. ISMA 1.0 is a standard for implementing MPEG-4 streaming media in the Internet, while ISMACryp 1.0 adds cryptographic mechanisms for enabling DRM to the ISMA standard. Since ISMACryp 1.0 satisfies requirements for Internet streaming and copyright protection, it is appropriate for playing DRM-enabled digital contents on the Internet. The digital contents to which ISMACryp 1.0 is applied can be replayed both in the IP set-top box and personal computer. The IP set-top box is a device that is subsidiary to television for various broadcasting services, and is expected as an essential element in a home networking environments. Nowadays, it is a trend to make the IP set-top box as a multi purpose device that is vary similar to personal computer. We could also prospect that the IP set-top box replaces the personal computer as a major client system for streaming services. We design and implement the secure DRM client system for playing ISMACryp-enabled digital contents. Especially, we develop the lightweight SecureDB and SecureDB Daemon for protecting sensitive information such as cryptographic keys. We also apply them to the commercialized embedded Linux IP set-top box for enabling the secure contents distribution system. [J650]

"Digital rights management"

Digital rights management broadly refers to a set of policies, techniques and tools that guide the proper use of digital content. A DRM plays important roles in several processes that are involved in the flow of content. The major functionalities of this DRM system are: packaging of the raw content for easy distribution and tracking, content protection for tamper-proof transmission, delivery of content offline on CDs and DVDs and delivering content on-demand over peer-to-peer networks. Thus a set of standards related to various aspects of DRM are practiced in order to ensure fairness, interoperability and also for the consumer confidence. [J651]

"Passwords and Passion"

A recent survey conducted by Sophos (www.sophos.com/pressoffice/news/articles/2006/04/passwordadvice.html) asked, "Do you use the same password for multiple Web sites?" Their admittedly unscientific results confirmed what most of us would expect: 41 percent of the respondents said they always use the same password, 45 percent said they have a few different passwords, and 14 percent said they never use the same password on multiple Web sites. Those 14 percent probably either don't have an Internet connection or are "security professionals." The problem is that where the "security professional" sees prudent, responsible behavior, users simply see overhead that gets in the way of performing whatever task they're trying to do. [J652]

"Scheduling security-critical real-time applications on clusters"

Security-critical real-time applications such as military aircraft flight control systems have mandatory security

requirements in addition to stringent timing constraints. Conventional real-time scheduling algorithms, however, either disregard applications' security needs and thus expose the applications to security threats or run applications at inferior security levels without optimizing security performance. In recognition that many applications running on clusters demand both real-time performance and security, we investigate the problem of scheduling a set of independent real-time tasks with various security requirements. We build a security overhead model that can be used to reasonably measure security overheads incurred by the security-critical tasks. Next, we propose a security-aware real-time heuristic strategy for clusters (SAREC), which integrates security requirements into the scheduling for real-time applications on clusters. Further, to evaluate the performance of SAREC, we incorporate the earliest deadline first (EDF) scheduling policy into SAREC to implement a novel security-aware real-time scheduling algorithm (SAEDF). Experimental results from both real-world traces and a real application show that SAEDF significantly improves security over three existing scheduling algorithms (EDF, least laxity first, and first come first serve) by up to 266.7 percent while achieving high schedulability. [J653]

"Information Ethics: Privacy and Intellectual Property"

{no data available} [J654]

"Dynamic software security testing"

Current software security techniques aren't able to produce the secure systems demanded by our increasingly interconnected society, so there persists the need for a more effective and scalable approach: dynamic software security testing [J655]

"The fourth amendment and emerging communications technologies"

The key US Supreme Court case that addresses the constitutionality of government surveillance is nearly four decades old. This overview considers how technological developments have strained the prevailing legal framework and highlights areas for reform [J656]

"Lost in translation: theory and practice in cryptography"

The perils of using encryption without authentication or integrity protection are well known in the cryptographic research community. Yet its exactly the mandatory support for unauthenticated encryption that forms the basis of a serious security flaw in an IPsec implementation we recently discovered. In response, the UK's equivalent to CERT, the National Infrastructure Coordination Centre published a vulnerability advisory about the flaw. Vendors also issued updated recommendations to customers, and we saw a flurry of discussion on Slash-dot and the sci.crypt newsgroup. In the aftermath, we asked ourselves, how did this happen? [J657]

"Progressive image transmission over space-time coded OFDM-based MIMO systems with adaptive modulation"

This paper considers a progressive image transmission system over wireless channels by combining joint source-channel coding (JSCC), space-time coding, and orthogonal frequency division multiplexing (OFDM). The BER performance of the space-time coded OFDM-based MIMO system based on a newly built broadband MIMO fading model is first evaluated by assuming perfect channel state information at the receiver for coherent detection. Then, for a given average SNR (hence, BER), a fast local search algorithm is applied to optimize the unequal error protection design in JSCC, subjected to fixed total transmitted energy for various constellation sizes. This design allows the measurement of the expected reconstructed image quality. With this end-to-end system performance evaluation, an adaptive modulation scheme is proposed to pick the constellation size that offers the best reconstructed image quality for each average SNR. Simulation results of practical image transmissions confirm the effectiveness of our proposed adaptive modulation scheme [J658]

"Data mining reactor fuel grab load trace data to support nuclear core condition monitoring"

A critical component of an advanced-gas cooled reactor (AGR) station is the graphite core. As a station ages, the graphite bricks that comprise the core can distort and may eventually crack. As the core cannot be replaced the core integrity ultimately determines the station life. Monitoring these distortions is usually restricted to the routine outages, which occur every few years, as this is the only time that the reactor core can be accessed by external sensing equipment. However, during weekly refueling activities measurements are taken from the core for protection and control purposes. It is shown in this paper that these measurements may be interpreted for condition monitoring purposes, thus potentially providing information relating to core condition on a more frequent basis. This paper describes the data-mining approach adopted to analyze this data and also describes a software system designed and implemented to support this process. The use of this software to develop a model

of expected behavior based on historical data, which may highlight events containing unusual features possibly indicative of brick cracking, is also described. Finally, the implementation of this newly acquired understanding in an automated analysis system is described. [J659]

"A joint signal processing and cryptographic approach to multimedia encryption"

In recent years, there has been an increasing trend for multimedia applications to use delegate service providers for content distribution, archiving, search, and retrieval. These delegate services have brought new challenges to the protection of multimedia content confidentiality. This paper discusses the importance and feasibility of applying a joint signal processing and cryptographic approach to multimedia encryption, in order to address the access control issues unique to multimedia applications. We propose two atomic encryption operations that can preserve standard compliance and are friendly to delegate processing. Quantitative analysis for these operations is presented to demonstrate that a good tradeoff can be made between security and bitrate overhead. In assisting the design and evaluation of media security systems, we also propose a set of multimedia-oriented security scores to quantify the security against approximation attacks and to complement the existing notion of generic data security. Using video as an example, we present a systematic study on how to strategically integrate different atomic operations to build a video encryption system. The resulting system can provide superior performance over both generic encryption and its simple adaptation to video in terms of a joint consideration of security, bitrate overhead, and friendliness to delegate processing. [J660]

"Resilient multicast conversational video"

We propose a feedback-based protocol for resilient multicast videoconferencing in error-prone networks. Unlike previous approaches, our scheme not only improves video quality at error-prone receivers, but it also maximizes the overall video quality of the session and achieves efficient usage of the available bandwidth. This protocol uses a decentralized repair request algorithm with (i) a new multicast suppression technique that protects critical correction requests and eliminates duplicated or overlapped control packets, and (ii) a new error resilience scheme based on multicast repair packets that convey predictive correction information to the video session. We present experimental videoconferencing results that demonstrate the effectiveness of the protocol in ad hoc WLANs [J661]

"Resource allocation with service differentiation for wireless video transmission"

The next generation wireless networks need to support video traffic. A major challenge in video services over wireless networks is quality of service (QoS) provisioning. Service differentiation is a good approach for QoS provisioning to video traffic. In this paper, we propose cross-layer protocol stack architecture for wireless video transmission with service differentiation. In the cross-layer architecture, the application layer provides the lower link layer with the video compression information. Using the information, a dynamic-weight generalized processor sharing (DWGPS) discipline is proposed for the link layer resource allocation. The link layer tries to provide the application layer with a stringent delay bound and strong protection to high priority traffic in the case of resource shortage. Acceptable level of fairness can be achieved by DWGPS. A scheduling procedure for DWGPS is presented, which avoids complex per-packet virtual time calculation. It is shown that DWGPS can automatically adapt to multiuser diversity without many modifications. Simulation results demonstrate the effectiveness and efficiency of the link-layer DWGPS resource allocation [J662]

"Unequal error protection for convolutional codes"

In this correspondence, unequal error-correcting capabilities of convolutional codes are studied. For errors in the information symbols and code symbols, the free input- and output-distances, respectively, serve as "unequal" counterparts to the free distance. When communication takes place close to or above the channel capacity the error bursts tend to be long and the free distance is not any longer useful as the measure of the error correcting capability. Thus, the active burst distance for a given output and the active burst distance for a given input are introduced as "unequal" counterparts to the active burst distance and improved estimates of the unequal error-correcting capabilities of convolutional codes are obtained and illustrated by examples. Finally, it is shown how to obtain unequal error protection for both information and code symbols using woven convolutional codes. [J663]

"On an upper bound for mixed error-correcting codes"

A mixed code is an error-correcting code in which different entries of the codewords can be chosen from different alphabets. In this correspondence an upper bound is given for the number of codewords in a mixed code where all the entries can come from distinct alphabets. This bound improves the sphere packing bound in several directions. The result is specialized to a simpler form in the case when only two distinct alphabets are used. Numerical results are presented to show that, in various cases, two different forms of the bound and

alternative choices of a parameter may give the strongest bound. [J664]

"A developmental view of system security"

Security policy can't be timeless, static, and universal. Security is more of a developmental problem than a technical one. Security should be integrated into an organization in such a way as to enhance and safeguard each facet in the least intrusive yet most effective way possible at a given time. Gradually, as the organization and the technology it uses "grow up together," security should become less intrusive, until at some point it's almost invisible. This article presents a developmental view of system security. [J665]

"Scalable authentication of MPEG-4 streams"

This paper presents three scalable and efficient schemes for authenticating MPEG-4 streams: the Flat Authentication Scheme, the Progressive Authentication Scheme, and the Hierarchical Authentication Scheme. All the schemes allow authentication of MPEG-4 streams over lossy networks by integrating seamlessly digital signatures and erasure correction coding with MPEG-4's fine granular scalability. A prominent feature of our schemes is their "sign once, verify many ways" property, i.e., they generate only one digital signature per compressed MPEG-4 object group, but allow clients to verify the authenticity of any down-scaled version of the original signed object group. [J666]

"The minimum distance problem for two-way entanglement purification"

Entanglement purification takes a number of noisy EPR pairs |00>+|11>and processes them to produce a smaller number of more reliable pairs. If this is done with only a forward classical side channel, the procedure is equivalent to using a quantum error-correcting code (QECC). We instead investigate entanglement purification protocols with two-way classical side channels (2-EPPs) for finite block sizes. In particular, we consider the analog of the minimum distance problem for QECCs, and show that 2-EPPs can exceed the quantum Hamming bound and the quantum Singleton bound. We also show that 2-EPPs can achieve the rate k/n=1-(t/n)log23-h(t/n)-O(1/n) (asymptotically reaching the quantum Hamming bound), where the EPP produces at least k good pairs out of n total pairs with up to t arbitrary errors, and h(x)=-xlog2x-(1-x)log2(1-x) is the usual binary entropy. In contrast, the best known lower bound on the rate of QECCs is the quantum Gilbert-Varshamov bound k/n≥1-(2t/n)log23-h(2t/n). Indeed, in some regimes, the known upper bound on the asymptotic rate of good QECCs is strictly below our lower bound on the achievable rate of 2-EPPs. [J667]

"Joint antenna selection and link adaptation for MIMO systems"

Multi-input multi-output (MIMO) systems, with multiple antennas at both the transmitter and the receiver, are anticipated to be widely employed in future wireless networks due to their predicted tremendous system capacity. To protect the transmitted data against random channel impairment, it is desirable to consider link adaptation, such as rate adaptation and power control, to improve the system performance and guarantee certain quality of service. Based on the observation that link adaptation and antenna selection problems are often coupled, we propose a joint antenna subset selection and link adaptation study for MIMO systems. After the formulation of the multidimensional joint optimization problem, the main contribution of this paper lies in the design of efficient algorithms approaching the optimal solution for both uncorrelated and correlated MIMO channels. Specifically, we propose one simplified antenna selection and link adaptation rule based on the expected optimal number of active antennas for uncorrelated MIMO with Rayleigh fading and one for correlated MIMO channels only based on the slowly varying channel correlation information. Our proposed algorithms are verified through numerical results, demonstrating significant gains over traditional MIMO signaling, while feasible for practical implementation. [J668]

"Digital rights management, spyware, and security"

In October 2005, Sysinternals' Mark Russinovich discovered a rootkit on his computer, which he later determined stemmed from a Sony-BMG compact disc. In this article, the authors examine the copy-protection software found on those discs and the implications for digital rights management. [J669]

"Ethical values of IT professionals: evidence from Hong Kong"

In the wake of recent scandals involving information technology (IT) professionals, the ethics of this profession deserve more attention. This paper reports on the first phase of an initiative to research the ethics of IT professionals. The ethical values of the IT profession in Hong Kong were investigated using an instrument designed to reflect the stages of moral reasoning present in Kohlberg's theory of Cognitive Moral Development. The vast majority of respondents espoused ethical values consistent with both a high level of reasoning and the

prevailing societal culture. At the same time, many respondents exhibited considerable uncertainty in their ethical reasoning, indicating a dynamic tension between high and low moral principles. The implications of these findings for research and practice are discussed. [J670]

"Recovery of the control plane after failures in ASON/GMPLS networks"

A reliable control plane plays a crucial role in creating high-level services in the next-generation transport network based on the generalized multiprotocol label switching (GMPLS) or automatically switched optical networks (ASON) model. Approaches to control-plane survivability, based on protection, and restoration mechanisms, are examined. Procedures for the control plane state recovery are discussed, including link and node failure recovery [J671]

"Examining coding structure and redundancy in DNA"

A review of DNA signal content, redundancy, and mutational mechanisms is presented. Mutation-robust methods are developed to detect a linear coding structure and approximate tandem repeats. In this article, a method to uncover an error-correction coding structure in the nucleotide sequence is developed and its efficiency in detecting approximate tandem repeats, such as microsatellite regions, is demonstrated. [J672]

"Rate-distortion optimized hybrid error control for real-time packetized video transmission"

The problem of application-layer error control for real-time video transmission over packet lossy networks is commonly addressed via joint source-channel coding (JSCC), where source coding and forward error correction (FEC) are jointly designed to compensate for packet losses. In this paper, we consider hybrid application-layer error correction consisting of FEC and retransmissions. The study is carried out in an integrated joint source-channel coding (IJSCC) framework, where error resilient source coding, channel coding, and error concealment are jointly considered in order to achieve the best video delivery quality. We first show the advantage of the proposed IJSCC framework as compared to a sequential JSCC approach, where error resilient source coding and channel coding are not fully integrated. In the IJSCC framework, we also study the performance of different error control scenarios, such as pure FEC, pure retransmission, and their combination. Pure FEC and application layer retransmissions are shown to each achieve optimal results depending on the packet loss rates and the round-trip time. A hybrid of FEC and retransmissions is shown to outperform each component individually due to its greater flexibility. [J673]

"Optimized transmission of JPEG2000 streams over wireless channels"

The transmission of JPEG2000 images over wireless channels is examined using reorganization of the compressed images into error-resilient, product-coded streams. The product-code consists of Turbo-codes and Reed-Solomon codes which are optimized using an iterative process. The generation of the stream to be transmitted is performed directly using compressed JPEG2000 streams. The resulting scheme is tested for the transmission of compressed JPEG2000 images over wireless channels and is shown to outperform other algorithms which were recently proposed for the wireless transmission of images. [J674]

"Mobility helps peer-to-peer security"

We propose a straightforward technique to provide peer-to-peer security in mobile networks. We show that far from being a hurdle, mobility can be exploited to set up security associations among users. We leverage on the temporary vicinity of users, during which appropriate cryptographic protocols are run. We illustrate the operation of the solution in two scenarios, both in the framework of mobile ad hoc networks. In the first scenario, we assume the presence of an offline certification authority and we show how mobility helps to set up security associations for secure routing; in this case, the security protocol runs over one-hop radio links. We further show that mobility can be used for the periodic renewal of vital security information (e.g., the distribution of hash chain/Merkle tree roots). In the second scenario, we consider fully self-organized security: Users authenticate each other by visual contact and by the activation of an appropriate secure side channel of their personal device; we show that the process can be fuelled by taking advantage of trusted acquaintances. We then show that the proposed solution is generic: It can be deployed on any mobile network and it can be implemented either with symmetric or with asymmetric cryptography. We provide a performance analysis by studying the behavior of the solution in various scenarios. [J675]

"Fingerprint multicast in secure video streaming"

Digital fingerprinting is an emerging technology to protect multimedia content from illegal redistribution, where each distributed copy is labeled with unique identification information. In video streaming, huge amount of data

have to be transmitted to a large number of users under stringent latency constraints, so the bandwidth-efficient distribution of uniquely fingerprinted copies is crucial. This paper investigates the secure multicast of anticollusion fingerprinted video in streaming applications and analyzes their performance. We first propose a general fingerprint multicast scheme that can be used with most spread spectrum embedding-based multimedia fingerprinting systems. To further improve the bandwidth efficiency, we explore the special structure of the fingerprint design and propose a joint fingerprint design and distribution scheme. From our simulations, the two proposed schemes can reduce the bandwidth requirement by 48% to 87%, depending on the number of users, the characteristics of video sequences, and the network and computation constraints. We also show that under the constraint that all colluders have the same probability of detection, the embedded fingerprints in the two schemes have approximately the same collusion resistance. Finally, we propose a fingerprint drift compensation scheme to improve the quality of the reconstructed sequences at the decoder's side without introducing extra communication overhead. [J676]

"Experience of numerical protective relays operating in an environment with high-frequency switching surge in Japan"

This paper intends to provide general information about the experiences of numerical relay operation under many different kinds of surges from switchyards in Japan. The main focus of this paper is to investigate the immunity of numerical relays against a switching surge with relatively high frequency in a gas-insulated substation that is considered to be severe for the relay's correct operation. It is concluded that the reliability of today's numerical relays in Japan against the switching surge is almost sufficient due to the effectiveness of the immunity test standard adopted and countermeasures against the switching surge in Japan. [J677]

"Modelling and control of agent-based power protection systems using supervisors"

The framework of supervisory control of discrete event systems (DESs) is applied to agent-based power protection systems for achieving high reliability and selectivity. The DES-based supervisory control uses feedback information of events occurring in systems to achieve the set of desired event sequences. The large-scale and complex power systems need systematic tools for protection and control on a more abstract level. The supervisory control technique on the event-based abstract level can be used as a formal method for protection of large-scale power systems. Specifically, a design procedure of a supervisor that coordinates the behaviour of relay agents to isolate fault areas through the minimum operations of circuit breakers is presented. [J678]

"Progressive quantized projection approach to data hiding"

A new image data-hiding technique is proposed. The proposed approach modifies blocks of the image after projecting them onto certain directions. By quantizing the projected blocks to even and odd values, one can represent the hidden information properly. The proposed algorithm performs the modification progressively to ensure successful data extraction without the need for the original image at the receiver side. Two techniques are also presented for correcting scaling and rotation attacks. The first approach is an exhaustive search in nature, which is based on a training sequence that is inserted as part of the hidden information. The second approach uses wavelet maxima as image semantics for rotation and scaling estimation. Both algorithms have proved to be effective in correcting rotation and scaling distortion. [J679]

"Inherent transient recovery voltage of power transformers-a model-based determination procedure"

Knowledge of the inherent transient recovery voltage (TRV) associated with power-transformer terminal faults is essential for correct application of circuit breakers. Instead of establishing standards for TRV parameters as a function of power transformer ratings, standardized model-based determination procedures are proposed. The dynamic properties of the transformer short-circuit impedance Zxallow a straightforward calculation of the TRV waveshape without high computational effort. Test setups for lightning impulse (LI), frequency response analysis (FRA) and low-voltage current injection (LVCI) are presented and discussed. A sample calculation introduces the TRV calculation from LI test data and comparison with LVCI and FRA results. It is concluded that the presented procedure should be incorporated into the transformer type-test routines to provide highly valuable information about the TRV of each specific transformer. [J680]

"On joint coding for watermarking and encryption"

In continuation of earlier work, where the problem of joint information embedding and lossless compression (of the composite signal) was studied in the absence and in the presence of attacks, here we consider the additional ingredient of protecting the secrecy of the watermark against an unauthorized party, which has no

access to a secret key shared by the legitimate parties. In other words, we study the problem of joint coding for three objectives: information embedding, compression, and encryption. Our main result is a coding theorem that provides a single-letter characterization of the best achievable tradeoffs among the following parameters: the distortion between the composite signal and the covertext, the distortion in reconstructing the watermark by the legitimate receiver, the compressibility of the composite signal (with and without the key), and the equivocation of the watermark, as well as its reconstructed version, given the composite signal. In the attack-free case, if the key is independent of the covertext, this coding theorem gives rise to a threefold separation principle that tells that asymptotically, for long block codes, no optimality is lost by first applying a rate-distortion code to the watermark source, then encrypting the compressed codeword, and finally, embedding it into the covertext using a previously proposed embedding scheme. In the more general case, however, this separation principle is no longer valid, as the key plays an additional role of side information used by the embedding unit [J681]

"Protecting job seekers from identity theft"

In search of a job after graduating from college, Meg Kemp posts her resume online. Norton Steuben, a retired law professor, hasn't looked for employment in more than 35 years and rarely uses the Internet, yet his law school maintains his curriculum vita online. Although such activity might seem innocuous, information in both these online resumes initially put Meg and Norton in danger of becoming identity-theft victims. Fortunately, they received some unexpected protection in the form of a computer program called Identity Angel, which this article describes in more detail. [J682]

"Calculation of transient radiation field from metallic enclosure of GIS based on surface-patch model"

To improve the computation accuracy of the transient radiation fields in gas insulated substation (GIS), surface-patch model is proposed in this paper, and the method of vector fitting combining with recursive convolution is applied to substitute the method of fast Fourier transform (FFT) in the process of field calculation. The transient radiation fields of an actual 125-kV GIS are calculated to confirm the correctness of the model and the method. It is seemed from the simulation that the method of vector fitting combining with recursive convolution can overcome the conventional problems of FFT and reduces the computer memory and CPU time successfully, and the results from surface-patch model are more accurate than those from thin-line model [J683]

"Some restrictions on weight enumerators of singly even self-dual codes"

In this correspondence, we give some restrictions on weight enumerators of singly even self-dual [n,n/2,d] codes whose shadows have minimum weight d/2. As a consequence, we determine the weight enumerators for which there is an extremal singly even self-dual [40,20,8] code and an optimal singly even self-dual [50,25,10] code [J684]

"Uncommon law [Jcopyright laws]"

This paper describes the non-profit organization established by the founder of Stanford Law School's Center for Internet and Society, Lawrence Lessig, that allows copyright holders grant flexible use of their work. Called Creative Commons, the organization simplifies the copyright law by enabling and encouraging people to become legal creators if they wanted to incorporate existing material. It facilitates the permissions that the copyright system before a user is allowed to build or share work. Copyright holders benefit primarily by having their work made accessible and encouraging others to build on their work. Engineers, meanwhile, benefit from access to vast information and instructional data. [J685]

"Rights protection for discrete numeric streams"

Today's world of increasingly dynamic environments naturally results in more and more data being available as fast streams. Applications such as stock market analysis, environmental sensing, Web clicks, and intrusion detection are just a few of the examples where valuable data is streamed. Often, streaming information is offered on the basis of a nonexclusive, single-use customer license. One major concern, especially given the digital nature of the valuable stream, is the ability to easily record and potentially "replay" parts of it in the future. If there is value associated with such future replays, it could constitute enough incentive for a malicious customer (Mallory) to record and duplicate data segments, subsequently reselling them for profit. Being able to protect against such infringements becomes a necessity. In this work, we introduce the issue of rights protection for discrete streaming data through watermarking. This is a novel problem with many associated challenges including: operating in a finite window, single-pass, (possibly) high-speed streaming model, and surviving natural domain specific transforms and attacks (e.g., extreme sparse sampling and summarizations), while at the same time keeping data alterations within allowable bounds. We propose a solution and analyze its resilience to

various types of attacks as well as some of the important expected domain-specific transforms, such as sampling and summarization. We implement a proof of concept software (wms.*) and perform experiments on real sensor data from the NASA Infrared Telescope Facility at the University of Hawaii, to assess encoding resilience levels in practice. Our solution proves to be well suited for this new domain. For example, we can recover an over 97 percent confidence watermark from a highly down-sampled (e.g., less than 8 percent) stream or survive stream summarization (e.g., 20 percent) and random alteration attacks with very high confidence levels, often above 99 percent. [J686]

"Security for multimedia adaptation: architectures and solutions"

Multimedia content adaptation enables users with different access networks, client devices, and/or user profiles to access the same information source. However, content adaptation also introduces security implications. We conduct an in-depth investigation into the potential security issues involved and analyze general security architectures and requirements. In particular, we address the issue of where to place the security functions and how this affects functionality. [J687]

"Securing embedded systems"

A top-down, multiabstraction layer approach for embedded security design reduces the risk of security flaws, letting designers maximize security while limiting area, energy, and computation costs [J688]

"Disenrollment with perfect forward secrecy in threshold schemes"

In this correspondence, we propose a new model for threshold schemes with disenrollment capability (TSDC), to address the scenarios in which the ability of a coalition to construct future shared secrets is prohibited. Compared to existing TSDC models, our model provides forward secrecy by adding a constraint that the broadcast from the dealer is required to activate the reconstruction of any secret. We also present a TSDC model in which the dealer has the enhanced capability of disenrolling any subset of participants, to prevent the otherwise unnecessary rekey of the entire group when a large number of participants are compromised. We establish the lower bounds on the entropy of broadcast messages in both proposed models, as guidelines on constructing broadcast efficient schemes, and present bound achieving schemes. [J689]

"News: data-driven enterprise-slouching toward the semantic Web"

Many organizations are still trying to figure out how to build a mostly object-oriented Web services system. In explaining the semantic Web's enterprise possibilities, the author emphasizes the benefits of direct access to the data within applications rather than integrating the applications themselves. Some industry observers still see the semantic Web as a theoretician's dream. Enterprises are still trying to figure out how to integrate applications via Web services and service-oriented architectures, so asking them to begin drawing up semantic Web capable taxonomies anytime soon isn't realistic. The knowledge sharing that would entice enterprises would allow relational databases to directly import ontologies and rules just as easily as they use standard SQL insert, update, and delete statements. Ontologies can act as the glue between multiple information sources, providing a consistent view of all the information, augmenting it and filling in the gaps. The best route for success will be to stop emphasizing what the semantic Web might do in the future and work instead on practical steps to improve the architecture. [J690]

"Architectures for Bit-Split String Scanning in Intrusion Detection"

String matching is a critical element of modern intrusion detection systems because it lets a system make decisions based not just on headers, but actual content flowing through the network. Through careful codesign and optimization of an architecture with a new string matching algorithm, the authors show it is possible to build a system that is almost 12 times more efficient than the currently best known approaches [J691]

"SCAN: self-organized network-layer security in mobile ad hoc networks"

Protecting the network layer from malicious attacks is an important yet challenging security issue in mobile ad hoc networks. In this paper, we describe SCAN, a unified network-layer security solution for such networks that protects both routing and data forwarding operations through the same reactive approach. SCAN does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to the malicious nodes. In SCAN, local neighboring nodes collaboratively monitor each other and sustain each other, while no single node is superior to the others. SCAN also adopts a novel credit strategy to decrease its overhead as time evolves. In essence, SCAN exploits localized collaboration and information cross-validation to protect the network in a self-organized manner. Through both analysis and simulation results, we demonstrate

the effectiveness of SCAN even in a highly mobile and hostile environment. [J692]

"Achieving privacy in trust negotiations with an ontology-based approach"

The increasing use of Internet in a variety of distributed multiparty interactions and transactions with strong real-time requirements has pushed the search for solutions to the problem of attribute-based digital interactions. A promising solution today is represented by automated trust negotiation systems. Trust negotiation systems allow subjects in different security domains to securely exchange protected resources and services. These trust negotiation systems, however, by their nature, may represent a threat to privacy in that credentials, exchanged during negotiations, often contain sensitive personal information that may need to be selectively released. In this paper, we address the problem of preserving privacy in trust negotiations. We introduce the notion of privacy preserving disclosure, that is, a set that does not include attributes or credentials, or combinations of these, that may compromise privacy. To obtain privacy preserving disclosure sets, we propose two techniques based on the notions of substitution and generalization. We argue that formulating the trust negotiation requirements in terms of disclosure policies is often restrictive. To solve this problem, we show how trust negotiation requirements can be expressed as property-based policies that list the properties needed to obtain a given resource. To better address this issue, we introduce the notion of reference ontology, and formalize the notion of trust requirement. Additionally, we develop an approach to derive disclosure policies from trust requirements and formally state some semantics relationships (i.e., equivalence, stronger than) that may hold between policies. These relationships can be used by a credential requestor to reason about which disclosure policies he/she should use in a trust negotiation. [J693]

"A security analysis of the Internet Chess Club"

The Internet Chess Club (ICC) is a popular online chess server that started its existence in the early 1990s as the Internet chess server. Although the ICC Web site assures its users that the security protocol employed between the client and the server protects sensitive information, the authors show that this isn't true. This article examines two security aspects of the ICC. In moving from a free service to a commercial one, ICC's administrators introduced several enhancements to the original system, including time-stamping, a network security protocol, and online payments. [J694]

"Challenges in securing the domain name system"

Two main security threats exist for DNS in the context of query/response transactions. Attackers can spoof authoritative name servers responding to DNS queries and alter DNS responses in transit through man-in-the-middle attacks, and alter the DNS responses stored in caching name servers. The IETF has defined the digital signature-based DNSSEC for protecting DNS query/response transactions through a series of requests for comments. [J695]

"High-payload image steganography using two-way block matching"

This letter presents a novel image steganography method that utilizes a two-way block-matching procedure to search for the highest similarity block for each block of the important image. The bases and indexes obtained together with some not-well-matched blocks are recorded in the least significant bits of the cover image using a hop scheme. The method exhibits a high data payload, which reduces the storage and transmission-time requirements and also provides a method that prevents an observer from selectively blocking the transmission of the important image. [J696]

"Safe harbor and privacy protection: a looming issue for IT professionals"

The 25 European Union (EU) Member States require that their residents' personal information not be transferred to countries that do not protect that information adequately. In 2000, the EU ruled that the United States (US), through its voluntary Safe Harbor program, met that requirement. Since that time, however, the EU has charged that many US companies that claim to be in compliance with Safe Harbor policies are not. In this article, I report on a study of the privacy-policy statements of 20 randomly selected US companies that claim to be in compliance. Of the 20, 19 are not in compliance. This study argues that as EU Member States begin to examine Safe Harbor carefully, they are likely to force US companies to adhere to more stringent privacy policies. The burden of this adherence will be borne by US IT professionals. [J697]

"Securing the whole enterprise: business and legal issues"

This paper discussed the importance of securing information for the whole enterprise and the factors that contribute to the difficulty of maintaining information security in an enterprise. The paper also discussed the

consequences of failing to address information security and proposed an approach to address the problem [J698]

"The NTMAC for authentication of noisy messages"

This paper introduces a new construct, called the Noise Tolerant Message Authentication Code (NTMAC), for noisy message authentication. The NTMAC can tolerate a small number of errors, such as might be caused by a noisy communications channel. The NTMAC uses a conventional Message Authentication Code (MAC) in its constructions and it inherits the conventional MAC's resistance to forgeries. Furthermore, the NTMAC gives an indication of the number and locations of the errors. [J699]

"Electric utility responses to grid security issues"

This paper discusses the different initiatives that utility decision makers have set in place to address the vulnerability of the US power grid to physical and cyber attacks. One of the efforts to enhance grid security is EPRI's Infrastructure Security Initiative (ISI), which was designed to develop both prevention countermeasures and enhanced recovery capabilities. To protect against cyber attacks, several organizations were also established including the Computer Emergency Response Team (CERT) and the Process Control Systems Forum (PCSF). In addition, EPRI also launched the Energy Information Security (EIS) program to focus on computer-based security breaches. An industry-wide cybersecurity program alliance, called the PowerSec Initiative, was also formed to address the cyberthreat issue as it could impact electric utility operational and control equipment. [J700]

"Protecting Combinational Logic Synthesis Solutions"

Recently, design reuse has emerged as a dominant design and system-integration paradigm for modern systems on silicon. However, the intellectual-property-business model is vulnerable to many dangerous obstructions, such as misappropriation and copyright fraud. The authors propose a new method for intellectual-property protection that relies upon design watermarking at the combinational-logic-synthesis level. They introduce two protocols for embedding user- and tool-specific information into a logic network while performing multilevel logic minimization and technology mapping, two standard-optimization processes during logic synthesis. The hidden information can be used to protect both the design and the synthesis tool. The authors demonstrate that the difficulty of erasing or finding a valid signature in the synthesized design can be made arbitrarily computationally difficult. In order to evaluate the developed-watermarking method, the authors applied it to a standard set of real-life benchmarks, where high probability of authorship was achieved with negligible overhead on solution quality [J701]

"Modeling of Transformer Windings Under Very Fast Transient Overvoltages"

To calculate the overvoltages in transformer windings under very fast transient overvoltages (VFTOs) generated by switching operations in gas-insulated substation (GIS), a single-input and multiple-output circuit model, which is based on a multiconductor transmission line (MTL) model, is presented in this paper. The procedure to determine the transfer function is deduced. Vector fitting and recursive convolution are used to calculate the time domain response. The resonant frequencies and the location of the resonance are determined by an analysis of the amplitude-frequency response characteristics. For validation, the calculated results are compared with the measurements on a transformer winding model, and the results are found to be satisfactory [J702]

"`Print and Scan' Resilient Data Hiding in Images"

Print-scan resilient data hiding finds important applications in document security and image copyright protection. This paper proposes methods to hide information into images that achieve robustness against printing and scanning with blind decoding. The selective embedding in low frequencies scheme hides information in the magnitude of selected low-frequency discrete Fourier transform coefficients. The differential quantization index modulation scheme embeds information in the phase spectrum of images by quantizing the difference in phase of adjacent frequency locations. A significant contribution of this paper is analytical and experimental modeling of the print-scan process, which forms the basis of the proposed embedding schemes. A novel approach for estimating the rotation undergone by the image during the scanning process is also proposed, which specifically exploits the knowledge of the digital halftoning scheme employed by the printer. Using the proposed methods, several hundred information bits can be embedded into images with perfect recovery against the print-scan operation. Moreover, the hidden images also survive several other attacks, such as Gaussian or median filtering, scaling or aspect ratio change, heavy JPEG compression, and rows and/or columns removal [J703]

"Traitor-Within-Traitor Behavior Forensics: Strategy and Risk Minimization"

Multimedia security systems have many users with different objectives and they influence each other's performance and decisions. Behavior forensics analyzes how users with conflicting interests interact with and respond to each other. Such investigation enables a thorough understanding of multimedia security systems and helps the digital rights enforcer offer stronger protection of multimedia. This paper analyzes the dynamics among attackers during multiuser collusion. The colluders share not only the profit from the redistribution of multimedia but also the risk of being detected by the content owner, and an important issue in collusion is fairness of the attack (i.e., whether all attackers share the same risk) (e.g., whether they have the same probability of being detected). While they might agree so, some selfish colluders may break their fair-play agreement in order to further lower their risk. This paper investigates the problem of "traitors within traitors" in multimedia forensics, in an effort to formulate the dynamics among attackers and understand their behavior to minimize their own risk and protect their own interests. As the first work on the analysis of this colluder dynamics, this paper explores some possible strategies that a selfish colluder can use to minimize his or her probability of being caught. We show that processing his or her fingerprinted copy before multiuser collusion helps a selfish colluder further lower his or her risk, especially when the colluded copy has high resolution and good quality. This paper also investigates the optimal precollusion processing strategies for selfish colluders to minimize their risk under the quality constraints [J704]

"Secure Integration of Distributed Medical Data Using Mobile Agents"

This article is part of a special issue on Intelligent Agents in Healthcare. This article proposes a secure medical-information-gathering system based on mobile agents that overcomes traditional systems' data availability issues. Information availability is a major concern when the provision of care is at stake. Physicians make their decisions based on available information. Virtual electronic patient records (VEPRs) provide the necessary means for intra-institution data integration, enabling a single view of all patients' clinical information. Nevertheless, patients are mobile entities visiting multiple institutions during their life, leaving a trail of scattered information. This proposal is based on a mobile-agent system that provides IEEE-FIPA standardized interinstitution data discovery, transport, and integration for medical information. It combines traditional security schemes for protecting information with advanced agent-driven self-protection mechanisms and role-based access control. The system interacts with remote legacy applications, thus facilitating integration of clinical documents. Highly sensitive medical information can be brought where needed. [J705]

"Guest Editors' Introduction: Data Surveillance"

The guest editors discuss data surveillance. Proponents hope that data surveillance technology will be able to anticipate and prevent terrorist attacks, detect disease outbreaks, and allow for detailed social science research--all without the corresponding risks to personal privacy because machines, not people, perform the surveillance. [J706]

"Countering Terrorism through Information and Privacy Protection Technologies"

Security and privacy aren't dichotomous or conflicting concerns--the solution lies in developing and integrating advanced information technologies for counterterrorism along with privacy-protection technologies to safeguard civil liberties. Coordinated policies can help bind the two to their intended use. [J707]

"Watermarking Algorithm based on the DWT"

Watermarking is considered as a desirable alternative for copyright protection of digital materials such as images, video and audio. Two kinds of watermarking algorithms are usually used: the watermarking algorithms using pseudorandom patterns and those using visual recognizable patterns. The main advantage of watermarking algorithms embedding a visual recognizable pattern, which can be the owner or provider logotype, is that after the extraction process the pattern can be visually recognized and then identified. In general the visual recognizable patterns has a large impact and less ambiguity during the copyright claim process as compared with the random patterns, however the amount of information required by the visual recognizable pattern is much larger than the amount of information required by the pseudorandom one, and then to achieve imperceptibility and robustness of the watermark is more difficult. This paper proposes a discrete wavelet transform (DWT) based watermark embedding algorithm for visual recognizable pattern which uses the relation between the human visual system and the DWT for embedding the watermark is such way that it becomes imperceptible and robust. Evaluation results show the desirable features of proposed scheme. [J708]

"News"

Timely news briefs in security, privacy, and policy [J709]

"Education: Scholarship for Service"

The US government created the scholarship for service (SFS) program to address the diminishing number of information assurance professionals it employs. In January 2000, an executive order defined the national plan for information systems protection, which outlined five federal cyber service training and education initiatives, including SFS. The next year, the national science foundation began awarding grants for student scholarships to universities that qualified as centers of academic excellence in information assurance education. In this article, the author outlines both SFS in general and New Mexico Institute of Mining and Technology's specific program [J710]

"Multiple Image Watermarking Applied to Health Information Management"

Information technology advances have brought forth new challenges in healthcare information management, due to the vast amount of medical data that needs to be efficiently stored, retrieved, and distributed, and the increased security threats that explicitly have to be addressed. The paper discusses the perspectives of digital watermarking in a range of medical data management and distribution issues, and proposes a complementary and/or alternative tool that simultaneously addresses medical data protection, archiving, and retrieval, as well as source and data authentication. The scheme imperceptibly embeds in medical images multiple watermarks conveying patient's personal and examination data, keywords for information retrieval, the physician's digital signature for authentication, and a reference message for data integrity control. Experimental results indicate the efficiency and transparency of the scheme, which conforms to the strict requirements that apply to regions of diagnostic significance [J711]

"Iterative joint channel decoding of correlated sources"

In this article we exploit the potential correlation existing between multiple information sources to achieve additional coding gains from the channel codes used for data protection. We do not assume the existence of, nor do we use channel side-information at the receiver. Instead, empirical estimates of the cross-correlation are used in partial decoding steps in an iterative joint soft decoding paradigm. Experimental results suggest that relatively few iterations (2 to 4) are sufficient to reap significant gains using this approach specially when the sources are highly correlated. Finally, we provide analytical performance bounds of the proposed technique showing a close match with the simulation results at sufficiently high SNR [J712]

"TraX: a device-centric middleware framework for location-based services"

Location-based services turned out not to be the "next big thing" following the success stories of GSM and SMS. The reasons for this are manifold and range from inaccurate cellular positioning technologies to a lack of competition in this field, both being closely related to the fact that positioning is controlled by a network-centric approach where the mobile network operator has the unique selling point for making position data available to third parties. However, things change: small, low-cost GPS receivers, either attachable to mobile devices or even integrated, are enjoying great popularity since their recent inception and are expected to become a standard feature of cell phones in the near future. In conjunction with mobile packet data services, they provide a basis for device-centric LBS platforms, where position data can be obtained directly from the mobile device. In this article the device-centric LBS middleware TraX, which focuses particularly on position management, advanced functions for interrelating the position data of several targets, and privacy protection, is presented. Due to its generic and open design, TraX can be reused for a broad range of different LBSs and thus fosters service diversity and multiprovider environments, both of which are essential for making the next generation of LBSs a success [J713]

"Nonbinary Stabilizer Codes Over Finite Fields"

One formidable difficulty in quantum communication and computation is to protect information-carrying quantum states against undesired interactions with the environment. To address this difficulty, many good quantum error-correcting codes have been derived as binary stabilizer codes. Fault-tolerant quantum computation prompted the study of nonbinary quantum codes, but the theory of such codes is not as advanced as that of binary quantum codes. This paper describes the basic theory of stabilizer codes over finite fields. The relation between stabilizer codes and general quantum codes is clarified by introducing a Galois theory for these objects. A characterization of nonbinary stabilizer codes over Fqin terms of classical codes over Fq2is provided that generalizes the well-known notion of additive codes over F4of the binary case. This paper also derives lower and upper bounds on the minimum distance of stabilizer codes, gives several code constructions, and derives numerous families of stabilizer codes, including quantum Hamming codes, quadratic residue codes, quantum Melas codes, quantum Bose-Chaudhuri-Hocquenghem (BCH) codes, and quantum character codes. The puncturing theory by Rains is

generalized to additive codes that are not necessarily pure. Bounds on the maximal length of maximum distance separable stabilizer codes are given. A discussion of open problems concludes this paper [J714]

"Secure Location Verification Using Radio Broadcast"

Secure location verification is a recently stated problem that has a number of practical applications. The problem requires a wireless sensor network to confirm that a potentially malicious prover is located in a designated area. The original solution to the problem, as well as solutions to related problems, exploits the difference between propagation speeds of radio and sound waves to estimate the position of the prover. In this paper, we propose a solution that leverages the broadcast nature of the radio signal emitted by the prover and the distributed topology of the network. The idea is to separate the functions of the sensors. Some sensors are placed such that they receive the signal from the prover if it is inside the protected area. The others are positioned so that they can only receive the signal from the prover outside the area. Hence, the latter sensors reject the prover if they hear its signal. Our solution is versatile and it deals with provers using either omni-directional or directional propagation of radio signals without requiring any special hardware besides a radio transceiver. We estimate the bounds on the number of sensors required to protect the areas of various shapes and extend our solution to handle complex radio signal propagation, optimize sensor placement, and operate without precise topology information [J715]

"Reversible Steganography for VQ-Compressed Images Using Side Matching and Relocation"

The reversible steganographic method allows an original image to be completely reconstructed from the stegoimage after the extraction of the embedded data. The traditional reversible embedding schemes are not suitable for images compressed using vector quantization (VQ) and usually require the use of the location map for reversibility. In this paper, we propose a reversible embedding scheme for VQ-compressed images that is based on side matching and relocation. The new method achieves reversibility without using the location map. The experimental results show that the proposed method is practical for VQ-compressed images and provides high image quality and embedding capacity [J716]

"Some Compartmentalized Secure Task Assignment Models for Distributed Systems"

This paper formulates abstract problems of assigning subtasks to agents (processors) in a distributed system with a goal that they can perform its global task efficiently. The paper models the distributed system with a graph that describes the communication capabilities of the constituting agents. This graph is referred to as the "organizational graph." In addition, the desired task-performing activity is modeled with another graph describing the required communications. Then, a few variants of the task assignment problem are formulated with potentially conflicting objectives (or constraints) of load balancing and communication costs. For some of these variants this paper provides efficient algorithms that solve the assignment problem. Some problems are proven NP-complete, and some others are left open. [J717]

"Progressive Transmission of Images Over Fading Channels Using Rate-Compatible LDPC Codes"

In this paper, we propose a combined source/channel coding scheme for transmission of images over fading channels. The proposed scheme employs rate-compatible low-density parity-check codes along with embedded image coders such as JPEG2000 and set partitioning in hierarchical trees (SPIHT). The assignment of channel coding rates to source packets is performed by a fast trellis-based algorithm. We examine the performance of the proposed scheme over correlated and uncorrelated Rayleigh flat-fading channels with and without side information. Simulation results for the expected peak signal-to-noise ratio of reconstructed images, which are within 1 dB of the capacity upper bound over a wide range of channel signal-to-noise ratios, show considerable improvement compared to existing results under similar conditions. We also study the sensitivity of the proposed scheme in the presence of channel estimation error at the transmitter and demonstrate that under most conditions our scheme is more robust compared to existing schemes [J718]

"Computer Security Education and Research: Handle with Care"

In seeking ways to actively detect attackers and their malicious code and tools, researchers, educators, and their students must tread somewhat cautiously, to ensure that their own computing activities remain legal and ethical. Although the intent behind protecting and securing systems serves the overall societal good, the methods used to achieve these ends must remain both legal and ethical. These issues also make great classroom discussion topics in any information security curriculum. [J719]

"Are You Sure You Had a Privacy Incident?"

Stories about security breach are in the news. Some stories concern "leaks" of companies' sensitive information, the urgency of finding the source (or sources), and the efforts to interdict them or "plug" the leaks. But most published stories involve the loss of control over personal information stored in electronically saved records; they therefore often include whether there has been a privacy compromise. Whether its lost laptops, misplaced backup tapes, or data posted to Web sites, data spills have become a fact of life for all of us. In the US, state governments and federal agencies have responded with a series of notification rules, which require companies to inform the affected individuals after security incidents [J720]

"Systemic Security Management"

The University of Southern California's Institute for Critical Information Infrastructure Protection (ICIIP) developed a conceptual framework for enterprise security. ICIIP (which shouldn't be confused with the Institute for Information Infrastructure Protection, or I3P) sought to close the gap between the current corporate cybersecurity risk profile and what's needed to protect the US's critical infrastructure information. The ICIIP framework analyzes organizational systems (not computer systems, but rather coordinated organizational bodies), incorporates multiple disciplines, and makes recommendations about those systems' structure and relationships [J721]

"Guest Editors' Introduction: Data Surveillance"

The guest editors discuss data surveillance. Proponents hope that data surveillance technology will be able to anticipate and prevent terrorist attacks, detect disease outbreaks, and allow for detailed social science research--all without the corresponding risks to personal privacy because machines, not people, perform the surveillance. [J722]

"Countering Terrorism through Information and Privacy Protection Technologies"

This article describes a vision for countering terrorism through information and privacy-protection technologies. This vision was initially imagined as part of a research and development (R&D) agenda sponsored by DARPA in 2002 in the form of the information awareness office (IAO) and the total information awareness (TIA) program. It includes a critical focus and commitment to delicately balancing national security objectives with privacy and civil liberties. We strongly believe that the two don't conflict and that the ultimate solution lies in utilizing information technologies for counterterrorism along with privacy-protection technologies to safeguard civil liberties, and twining them together with coordinated policies that bind them to their intended use [J723]

"Strengthening the Weakest Link in Digital Protection"

Although much has been written about digital protection technologies, the greatest vulnerability in any system is invariably the person behind the keyboard. In our one-semester course at the US Military Academy in New York, we educate roughly 800 undergraduates from nontechnical fields each year on intermediate-level IT skills. We place our students in an isolated virtual-computing environment, give them hands-on experience with a variety of attack vectors that hackers use to exploit vulnerabilities, and provide them with a multidimensional framework for understanding and mitigating risks. As a result of this educational experience, our students are better able to internalize the concepts we teach and end up with an increased realization of the actions required to protect crucial resources. To achieve our goal of reducing the potential vulnerabilities nontechnical users introduce, we've integrated three major components into our course: 1) a broad overview of key IT topics; 2) lessons directly targeting information assurance (IA); and 3) a recurring thread of ethical and security considerations that's explicitly injected into lessons throughout the semester [J724]

"An ROV Stereovision System for Ship-Hull Inspection"

Ship hulls, as well as bridges, port dock pilings, dams, and various underwater structures need to be inspected for periodic maintenance. Additionally, there is a critical need to provide protection against sabotage activities, and to establish effective countermeasures against illegal smuggling activities. Unmanned underwater vehicles are suitable platforms for the development of automated inspection systems, but require integration with appropriate sensor technologies. This paper describes a vision system for automated ship-hull inspection, based on computing the necessary information for positioning, navigation, and mapping of the hull from stereo images. Binocular cues are critical in resolving a number of complex visual artifacts that hamper monocular vision in shallow-water conditions. Furthermore, they simplify the estimation of vehicle pose and motion, which is fundamental for successful automatic operation. The system has been implemented on a commercial remotely operated vehicle (ROV), and tested in pool and dock tests. Results from various trials are presented to demonstrate the system capabilities [J725]

"Techniques for integrating sensors into the enterprise network"

Cheap programmable sensor devices are becoming commercially available. They offer the possibility of transforming existing enterprise applications and enabling entirely new ones. The merging of sensor networks into the enterprise network poses some distinct problems. In particular, information from theses devices must be obtained in a way which minimizes their energy use and must be aggregated and filtered before being sent to the application server to prevent it from being overwhelmed. We describe a range of complementary techniques for integrating sensors into an enterprise network. These comprise new architectural entities within the enterprise network-edge server-new means of sharing information within the enterprise network-messaging binning-and new protocols for extracting information from the sensor network-Messo. [J726]

"Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents"

Secure communication of data over public channels is one of the most important challenges. Both the activities to secure contents and to break security are very hot. In order to reduce the chances of attack, security needs to be made invisible. The needs to preserve originality, ownership information, and integrity of text documents in a way that cannot be identified by everyone is being felt badly. Watermarking of the documents is a step toward achieving these objectives. However, to watermark a plain text document (ASCII) in a way that the original text will not change (and it would be very difficult to break it), is a great challenge. We have developed a novel encoding scheme which can be used to insert information in plain text without changing the text. A system has been developed based upon this encoding scheme. This paper describes the system and demonstrates its workings [J727]

"A Survey on Mix Networks and Their Secure Applications"

Anonymity is a subdiscipline of information hiding, required in a number of applications, such as in electronic voting. For network communications, anonymity can be provided by a mix network (mixnet). A mixnet is a multistage system that uses cryptography and permutations to provide anonymity. The basic idea of a mixnet has evolved into a number of different classes. In addition to presenting the existing mixnet classifications, this paper classifies mixnets based on the verification mechanisms employed for robustness. The construction of mixnets is presented under a common framework to provide insight into both the design and weaknesses of existing solutions. Basic forms of attack on mixnets and the corresponding robustness solutions are reviewed. Comparison with other solutions for anonymity and suggestions for interesting future research in mix networks are also provided [J728]

"Strengthening the Weakest Link in Digital Protection"

In our one-semester course at the US Military Academy in New York, we educate roughly 800 undergraduates from nontechnical fields each year on intermediate-level IT skills. We place our students in an isolated virtual-computing environment, give them hands-on experience with a variety of attack vectors that hackers use to exploit vulnerabilities, and provide them with a multidimensional framework for understanding and mitigating risks. As a result of this educational experience, our students are better able to internalize the concepts we teach and end up with an increased realization of the actions required to protect crucial resources. [J729]

"A survey of key management in ad hoc networks"

First Page of the Article [J730]

"Are You Sure You Had a Privacy Incident?"

Whether it's lost laptops, misplaced backup tapes, or data posted to Web sites, data spills have become a fact of life. In the US, state governments and federal agencies have responded with a series of notification rules, which require companies to inform the affected individuals after security incidents. Yet, to determine whether an incident affects individuals' privacy and thus requires notice, organizations must uncover a fairly in-depth set of facts. [J731]

"Systemic Security Management"

In 2005, the University of Southern California's Institute for Critical Information Infrastructure Protection (ICIIP) developed a conceptual framework for enterprise security. ICIIP seeks to close the gap between the current corporate cybersecurity risk profile and what's needed to protect the US's critical infrastructure information. [J732]

"News Briefs"

New Panel Aims to Identify Risks and Challenges; IPv6 to Influence $97 Billion in US Government Spending; Microsoft Debuts MySpace for IT; Report: New Hackers Up to Old Tricks; Study: People and Processes Important in Security; Internet Explorer 7 for Windows XP Available; Mozilla Releases Newest Firefox; MySQL Boosts Service Features for Enterprise Clients; Cisco Presents Next-Generation Virtual Meeting Technology; Dell Unveils Two- and Four-Socket Servers, Integrates Oracle; Sophos Confident in its Vista Protection; Microsoft to Release EU-Compliant Vista; EPA Announces New Computer Efficiency Requirements; Skype Introduces Video Calling for Mac Users, Aims for Legitimacy; Sony Recalls Additional Notebook Batteries. [J733]

"News Briefs"

New Panel Aims to Identify Risks and Challenges; IPv6 to Influence $97 Billion in US Government Spending; Microsoft Debuts MySpace for IT; Report: New Hackers Up to Old Tricks; Study: People and Processes Important in Security; Internet Explorer 7 for Windows XP Available; Mozilla Releases Newest Firefox; MySQL Boosts Service Features for Enterprise Clients; Cisco Presents Next-Generation Virtual Meeting Technology; Dell Unveils Two- and Four-Socket Servers, Integrates Oracle; Sophos Confident in its Vista Protection; Microsoft to Release EU-Compliant Vista; EPA Announces New Computer Efficiency Requirements; Skype Introduces Video Calling for Mac Users, Aims for Legitimacy; Sony Recalls Additional Notebook Batteries. [J734]

"News"

Timely news briefs in security, privacy, and policy [J735]

"Silicon Microdosimetry in Heterogeneous Materials: Simulation and Experiment"

Microdosimetry spectra obtained experimentally utilizing a Silicon-On-Insulator (SOI) microdosimeter within biological materials, was used to provide information on secondary radiation spectra at tissue boundaries. Comparative GEANT4 simulations of the experimental conditions were also conducted [J736]

"Book Reviews: Breaking Security Design Bottlenecks in Payment Technologies"

A review of Payment Technologies for E-Commerce by Weidong Kou, ed. [J737]

"Using SAML to protect the session initiation protocol (SIP)"

The security assertion markup language (SAML) standard supports the expression of security assertions such as authentication, role membership, or permissions. SAML assertions may be used to realize single-sign-on between Web servers located in different domains. After a short introduction to SAML, this article describes the application of SAML to protect session initiation protocol (SIP) signaling [J738]

"Managing information privacy: developing a context for security and privacy standards convergence"

Information privacy is much broader than data security. It's about the collection, processing, use, and protection of personal information. Essentially, business processes, IT systems, and compliance controls must support the full set of requirements embodied in these principles and expressed in relevant laws and policies. Implementation choices, including automation level and security control selection, become business and business-risk decisions. To institute such principles, businesses should understand the critical need for policy-driven security and privacy compliance in developing the right business processes and overall technical architecture [J739]

"Integrating Security Policies via Container Portable Interceptors"

Enforcing appropriate security policies in distributed, component-based applications is difficult. A generic framework to define and evaluate security policies is necessary, and that framework must be integrated with the middleware platform. The middleware must provide the necessary hooks to intercept calls and obtain the information required for security enforcement. We designed and developed a security framework, integrated it into the CORBA component model middleware platform, and evaluated it in a real-world project [J740]

"Kafka in the academy: a note on ethics in IA education"

In studying how to protect the United States' critical infrastructure, a presidential commission divided it into several sectors: information and communications, banking and finance, energy, physical distribution, and vital human services. Given that all sectors are strongly interconnected, the vulnerability of one represents dangers for the others. For example, a failure in the communications infrastructure would quickly have consequences in the

finance and physical distribution sectors, which rely on it for coordination. Disruption of finance and transportation would quickly spill over into the energy and human services sectors. The communications and information infrastructures' self-evident long-term dependence on energy and finance completes the cycle [J741]

"Lessons for laptops from the 18th century"

As governments attempt to prevent, investigate, or prosecute crimes by persons who use the Internet to plan and carry out terrorist acts, the protection of private, personal information stored on computers becomes the subject of controversy. It is inevitable that the home computer becomes a target for surveillance, search, and seizure by government agents. As a result, courts will be asked to determine whether such agents have complied with applicable laws that condition such intrusions on meeting standards set by constitutions or laws that did not anticipate the home computer as a focal point for such controversies. Courts are more accustomed to addressing similar controversies in the context of a house and its material contents, rather than a computer and its digital files. It is likely that the judicial system will use analogies to the house when deciding controversies concerning the reasonable expectations of privacy in a home computer's contents. In apparent anticipation, the US Justice Department's policy on the search and seizure of computers in investigations uses such an analogy to justify its position that when several people share a computer, any one of them can grant the police permission to search and seize its contents [J742]

"System Call Monitoring Using Authenticated System Calls"

System call monitoring is a technique for detecting and controlling compromised applications by checking at runtime that each system call conforms to a policy that specifies the program's normal behavior. Here, we introduce a new approach to implementing system call monitoring based on authenticated system calls. An authenticated system call is a system call augmented with extra arguments that specify the policy for that call, and a cryptographic message authentication code that guarantees the integrity of the policy and the system call arguments. This extra information is used by the kernel to verify the system call. The version of the application in which regular system calls have been replaced by authenticated calls is generated automatically by an installer program that reads the application binary, uses static analysis to generate policies, and then rewrites the binary with the authenticated calls. This paper presents the approach, describes a prototype implementation based on Linux and the PLTO binary rewriting system, and gives experimental results suggesting that the approach is effective in protecting against compromised applications at modest cost [J743]

"Dual protection of JPEG images based on informed embedding and two-stage watermark extraction techniques"

In this paper, the authors propose a watermarking scheme that embeds both image-dependent and fixed-part marks for dual protection (content authentication and copyright claim) of JPEG images. To achieve the goals of efficiency, imperceptibility, and robustness, a compressed-domain informed embedding algorithm, which incorporates the Lagrangian multiplier optimization approach and an adjustment procedure, is developed. A two-stage watermark extraction procedure is devised to achieve the functionality of dual protection. In the first stage, the semifragile watermark in each local channel is extracted for content authentication. Then, in the second stage, a weighted soft-decision decoder, which weights the signal detected in each channel according to the estimated channel condition, is used to improve the recovery rate of the fixed-part watermark for copyright protection. The experiment results manifest that the proposed scheme not only achieve dual protection of the image content, but also maintain higher visual quality (an average of 6.69 dB better than a comparable approach) for a specified level of watermark robustness. In addition, the overall computing load is low enough to be practical in real-time applications [J744]

"For the birds"

First Page of the Article [J745]

"Detecting and Isolating Malicious Routers"

Network routers occupy a unique role in modern distributed systems. They are responsible for cooperatively shuttling packets amongst themselves in order to provide the illusion of a network with universal point-to-point connectivity. However, this illusion is shattered-as are implicit assumptions of availability, confidentiality, or integrity-when network routers are subverted to act in a malicious fashion. By manipulating, diverting, or dropping packets arriving at a compromised router, an attacker can trivially mount denial-of-service, surveillance, or man-in-the-middle attacks on end host systems. Consequently, Internet routers have become a choice target for would-be attackers and thousands have been subverted to these ends. In this paper, we specify this problem of detecting routers with incorrect packet forwarding behavior and we explore the design space of protocols that

implement such a detector. We further present a concrete protocol that is likely inexpensive enough for practical implementation at scale. Finally, we present a prototype system, called Fatih, that implements this approach on a PC router and describe our experiences with it. We show that Fatih is able to detect and isolate a range of malicious router actions with acceptable overhead and complexity. We believe our work is an important step in being able to tolerate attacks on key network infrastructure components [J746]

"Behavior forensics for scalable multiuser collusion: fairness versus effectiveness"

Multimedia security systems involve many users with different objectives and users influence each other's performance. To have a better understanding of multimedia security systems and offer stronger protection of multimedia, behavior forensics formulate the dynamics among users and investigate how they interact with and respond to each other. This paper analyzes the behavior forensics in multimedia fingerprinting and formulates the dynamics among attackers during multi-user collusion. In particular, this paper focuses on how colluders achieve the fair play of collusion and guarantee that all attackers share the same risk (i.e., the probability of being detected). We first analyze how to distribute the risk evenly among colluders when they receive fingerprinted copies of scalable resolutions due to network and device heterogeneity. We show that generating a colluded copy of higher resolution puts more severe constraints on achieving fairness. We then analyze the effectiveness of fair collusion. Our results indicate that the attackers take a larger risk of being captured when the colluded copy has higher resolution, and they have to take this tradeoff into consideration during collusion. Finally, we analyze the collusion resistance of the scalable fingerprinting systems in various scenarios with different system requirements, and evaluate the maximum number of colluders that the fingerprinting systems can withstand [J747]

"Enhancing security using mobility-based anomaly detection in cellular mobile networks"

Location information is an important feature in users' profiles in cellular mobile networks. In this paper, by exploiting the location history traversed by a mobile user, two domain-independent online anomaly detection schemes are designed, namely the Lempel-Ziv (LZ)-based and Markov-based detection schemes. The authors focus on the identification of a group of especially harmful internal attackers-masqueraders. For both schemes, cell IDs traversed by each mobile user are extracted as the feature value. Specifically, the mobility pattern of each user is characterized by a high-order Markov model. The LZ-based detection scheme from the well-developed data compression techniques is derived. Moreover, the technique of exponentially weighted moving average is used to modify a user's normal profile dynamically. The user profile can characterize the normal behavior of each user accurately and is sensitive to abnormal changes. For the Markov-based detection scheme, a fixed-order Markov model is used to characterize the normal behavior. Based on the constructed probability transition matrix, the probability of the user's current activity is calculated. A threshold policy is then used in both schemes to determine whether a mobile device is potentially compromised or not. Simulation results are presented to show the effectiveness of the proposed schemes. Moreover, our results show that the LZ-based detection scheme performs better than the Markov-based detection scheme, especially for low-speed mobile users [J748]

"A Tree-Based Data Perturbation Approach for Privacy-Preserving Data Mining"

Due to growing concerns about the privacy of personal information, organizations that use their customers' records in data mining activities are forced to take actions to protect the privacy of the individuals. A frequently used disclosure protection method is data perturbation. When used for data mining, it is desirable that perturbation preserves statistical relationships between attributes, while providing adequate protection for individual confidential data. To achieve this goal, we propose a kd-tree based perturbation method, which recursively partitions a data set into smaller subsets such that data records within each subset are more homogeneous after each partition. The confidential data in each final subset are then perturbed using the subset average. An experimental study is conducted to show the effectiveness of the proposed method [J749]

"Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection"

The major disadvantage of existing watermarking methods is their limited resistance to extensive geometric attacks. In addition, we have found that the weakness of multiple watermark embedding methods that were initially designed to resist geometric attacks is their inability to withstand the watermark-estimation attacks (WEAs), leading to reduce resistance to geometric attacks. In view of these facts, this paper proposes a robust image watermarking scheme that can withstand geometric distortions and WEAs simultaneously. Our scheme is mainly composed of three components: 1) robust mesh generation and mesh-based watermarking to resist geometric distortions; 2) construction of media hash-based content-dependent watermark to resist WEAs; and 3)

a mechanism of false positive-oriented watermark detection, which can be used to determine the existence of a watermark so as to achieve a tradeoff between correct detection and false detection. Furthermore, extensive experimental results obtained using the standard benchmark (i.e., Stirmark) and WEAs, and comparisons with relevant watermarking methods confirm the excellent performance of our method in improving robustness. To our knowledge, such a thorough evaluation has not been reported in the literature before [J750]

"Joint source-channel coding for wireless object-based video communications utilizing data hiding"

In recent years, joint source-channel coding for multimedia communications has gained increased popularity. However, very limited work has been conducted to address the problem of joint source-channel coding for object-based video. In this paper, we propose a data hiding scheme that improves the error resilience of object-based video by adaptively embedding the shape and motion information into the texture data. Within a rate-distortion theoretical framework, the source coding, channel coding, data embedding, and decoder error concealment are jointly optimized based on knowledge of the transmission channel conditions. Our goal is to achieve the best video quality as expressed by the minimum total expected distortion. The optimization problem is solved using Lagrangian relaxation and dynamic programming. The performance of the proposed scheme is tested using simulations of a Rayleigh-fading wireless channel, and the algorithm is implemented based on the MPEG-4 verification model. Experimental results indicate that the proposed hybrid source-channel coding scheme significantly outperforms methods without data hiding or unequal error protection [J751]

"The MIMO ARQ Channel: Diversity–Multiplexing–Delay Tradeoff"

In this paper, the fundamental performance tradeoff of the delay-limited multiple-input multiple-output (MIMO) automatic retransmission request (ARQ) channel is explored. In particular, we extend the diversity-multiplexing tradeoff investigated by Zheng and Tse in standard delay-limited MIMO channels with coherent detection to the ARQ scenario. We establish the three-dimensional tradeoff between reliability (i.e., diversity), throughput (i.e., multiplexing gain), and delay (i.e., maximum number of retransmissions). This tradeoff quantifies the ARQ diversity gain obtained by leveraging the retransmission delay to enhance the reliability for a given multiplexing gain. Interestingly, ARQ diversity appears even in long-term static channels where all the retransmissions take place in the same channel state. Furthermore, by relaxing the input power constraint allowing variable power levels in different retransmissions, we show that power control can be used to dramatically increase the diversity advantage. Our analysis reveals some important insights on the benefits of ARQ in slow-fading MIMO channels. In particular, we show that 1) allowing for a sufficiently large retransmission delay results in an almost flat diversity-multiplexing tradeoff, and hence, renders operating at high multiplexing gain more advantageous; 2) MIMO ARQ channels quickly approach the ergodic limit when power control is employed. Finally, we complement our information-theoretic analysis with an incremental redundancy lattice space-time (IR-LAST) coding scheme which is shown, through a random coding argument, to achieve the optimal tradeoff(s). An integral component of the optimal IR-LAST coding scheme is a list decoder, based on the minimum mean-square error (MMSE) lattice decoding principle, for joint error detection and correction. Throughout the paper, our theoretical claims are validated by numerical results [J752]

"In the News"

The Web's inherent openness and potential for growth and new applications make it a powerful tool, especially as methods develop for handling data on the semantic Web. In the semantic Web, heterogeneous data sources can be treated as a single source, with an ontology that mediates between them, thereby allowing the creation of knowledge out of information. But formidable problems accompany its potential to publish and store massive amounts of information. As more users access and reason over the information on the Web, particularly in pursuit of creating more valuable knowledge, issues arise of securing and protecting personal information and of this information's accuracy and provenance. Computer scientists are addressing these problems, imagining and developing solutions that range from semantic firewalls to methods for monitoring and auditing the use of information [J753]

"Security policies and the software developer"

A wide range of legal and regulatory issues surround Web software development, including the need to protect consumer information. A good set of security policies limit company exposure. Understanding and implementing good policies is therefore as essential as implementing SSL. In this article, we consider two simple questions: why should software architects and developers work with corporate information security policies and, just as important, how? But first, a disclaimer: by virtue of this discussion, we inevitably have to consider relevant state and federal laws and regulations. However, this article isn't predominantly about the law and isn't meant to render legal advice. Instead, we hope to understand how policy compliance plays a pivotal role in obtaining

protection both under and from the law. This article doesn't provide an exhaustive study of all the relevant laws, but we cited some sources of further information [J754]

"On the Probability of Undetected Error for Overextended Reed–Solomon Codes"

Upper and lower bounds on the weight distribution of overextended Reed-Solomon (OERS) codes are derived, from which tight upper and lower bounds on the probability of undetected error for OERS codes are obtained for q-ary symmetric channels [J755]

"Postmortem analysis and data validation in the wake of the 2004 Athens blackout"

On July 12, 2004 at 12:39 local time, the south part of the Hellenic Interconnected Transmission System (including Athens) was split from the rest of the system and collapsed, driving consumers with a total load of 4500 MW into blackout. Technical information about the causes, the evolution, and the consequences of the blackout are presented in this paper. Some qualitative conclusions drawn immediately after the blackout are presented, as well as the results of further studies, including detailed simulations with corrected data, generator adjustments, and protection considerations [J756]

"Tamper Proofing by Design Using Generalized Involution-Based Concurrent Error Detection for Involutional Substitution Permutation and Feistel Networks"

Secure operation of cryptographic algorithms is critical to the success of secure transactions. Fault-based attacks that recover secret keys by deliberately introducing fault(s) in cipher implementations and analyzing the faulty outputs have been proven to be extremely powerful. Substitution permutation networks (SPN) and Feistel networks (FN) are the two important classes of symmetric block ciphers. Some SPN ciphers and all FN ciphers satisfy the involution property. A function F is an involution if F(F(x)) = x. In this paper, we investigate tamper proofing techniques that use low cost involution-based time redundancy concurrent error detection (CED) schemes for involutional SPN and FN symmetric block ciphers. We incorporated this tamper proofing by design technique in a hardware implementation of the 128-bit ANUBIS SPN cipher (an involution variant of the advanced encryption standard (AES)) and the 128-bit TwoFish FN cipher (an AES finalist). We performed fault simulation at both the algorithm and the gate level to show that the low-cost involution-based CED schemes, in addition to detecting all transient faults, can detect all single-bit permanent faults and > 99 percent of all multiple-bit permanent faults. Consequently, this low cost CED technique can protect the crypto device against differential fault analysis (DFA) attacks [J757]

"A Framework for Describing Block Cipher Cryptanalysis"

Block ciphers provide confidentiality by encrypting confidential messages into unintelligible form, which are irreversible without knowledge of the secret key used. During the design of a block cipher, its security against cryptanalysis must be considered. History has shown that a cipher designed without an adequate treatment of this would often lead to flaws and attacks by other researchers, sometimes devastatingly so. The problem for an aspiring cipher designer is that there are no standard texts on block cipher cryptanalysis because it is a fast changing field. The commonly available references are academic journals and conference proceedings, which may not be easy to grasp for researchers new to cryptanalysis. This paper presents the Xi framework, which is designed to compactly describe the block cipher cryptanalysis techniques regardless of their individual differences. This provides the cryptanalyst with a general framework to describe attacks on block ciphers, with the additional capabilities of allowing specification of the technical details of each different type of attack and of comparison of their respective strengths. Comparing different distinguishes in this framework also allows us to see natural generalizations and trigger nice open problems. We then show how to apply this Xi framework to the description of various attacks on popular and recent block ciphers [J758]

"Unsupervised event extraction within substations using rough classification"

Microprocessor technology, broader bandwidth communications, and cheaper storage medium have greatly improved the capability to process, transmit, and store the large quantities of data available in a substation. Intelligent electronic devices (IEDs) normally acquire some of these data as raw facts, which then need to be interpreted in order to extract the useful information that engineers and operators require. Human interpretation is becoming increasingly impractical and the effect can hamper, or even prevent, an operator responding correctly to an emergency. This paper explains how a rough classification technique enhances the capabilities of substation informatics and provides valuable insight into the information contained in a substation dataset. This paper emphasizes postfault analysis of the protection and breaker responses in a substation. It is designed to help the operator understand overwhelming alarm messages or longer term to help engineers analyze what went wrong. The formulated methodology is generic and applicable to any type of transmission and distribution

substation [J759]

"Using Battery Constraints within Mobile Hosts to Improve Network Security"

Distributed battery-based intrusion detection (B-BID) is an efficacious early-warning system that can complement existing intrusion detection systems (IDSs) by alerting users to protect their mobile devices as well as network administrators to protect their corporate networks by correlating device power consumption with application and attack activity data [J760]

"Toward Secure Routing Infrastructures"

The protocols, data, and algorithms that compute paths through interconnected network devices are possibly the most vital, complex, and fragile components in the global information infrastructure. They are also the least protected. This article examines the current state of, and practical prospects for, security in IP routing infrastructures [J761]

"A microcomputer-based unique digital fault diagnosis scheme of radial transformer feeders"

This investigation aims to develop a comprehensive microcomputer based fault protection scheme for indicating various types of faults in a radial transformer feeder in subtransmission or distribution circuits and its protection against those faults. The type of fault in the feeder can also be determined by observing the phase angles of the primary currents of the transformer with which the feeder is connected at its secondary. This method dispenses off conventional electromagnetic relays and HRC fuses in feeder protection schemes. The developed system provides necessary information regarding the faulted phase and displays appropriate symbols on the display screen of the microcomputer about the type of fault [J762]

"Securing voice over IP"

{no data available} [J763]

"Information leak vulnerabilities in SIP implementations"

The use of VoIP as a cheaper communications alternative is growing at an astronomical rate. However, potential abuse of the technology may hinder its deployment. One key security concern is the exploitation of implementation vulnerabilities in the form of unauthorized access, worms, viruses, and denial of service attacks, particularly when combined with explicit targeting of implementations that are known to be vulnerable. One way to protect from exploitations of implementation-specific vulnerabilities is "security-by-obscurity" where a SIP device does not reveal its specific software version. For the same reason, the SIP standard does not encourage announcing the software version in SIP messages. In this article we show that even when SIP messages do not explicitly contain software version information, there is sufficient information leak to determine it. To demonstrate this, we introduce techniques to fingerprint SIP devices and develop a fingerprinting tool called SIPProbe that collects fingerprints and identifies SIP implementations. This type of information leak presents a new security concern as it can be used by malicious users as a building block to scan SIP devices and launch attacks [J764]

"A discrete Fourier transform-based adaptive mimic phasor estimator for distance relaying applications"

In protection relaying schemes, the digital filter unit plays the essential roles to calculate the accurate phasor. However, while the fault current contains plentiful decaying dc component, the over-reach of distance protection will cause sever problem. This work develops an adaptive mimic phasor estimator to remove the decaying dc oscillation between voltage and current and obtains the accurate apparent impedance. First, a discrete Fourier transform-based mimic phasor estimator is developed. Then, an adaptive scheme is proposed to obtain the decaying time constant. Unlike the fixed decaying dc time constant used in a digital mimic filter, the proposed algorithm adopts the transmission-line parameters information hiding in the voltage and current measurements to adaptively approximate the decaying dc time constant to the accurate value. Thus, the estimation error in the mimic filter due to the time constant mismatch can be eliminated. Both full-cycle and half-cycle versions are developed in this work. Simulations results illustrate the effectiveness of this new algorithm for distance relaying applications [J765]

"Adaptive Defense Against Various Network Attacks"

In defending against various network attacks, such as distributed denial-of-service (DDoS) attacks or worm attacks, a defense system needs to deal with various network conditions and dynamically changing attacks.

Therefore, a good defense system needs to have a built-in "adaptive defense" functionality based on cost minimization-adaptively adjusting its configurations according to the network condition and attack severity in order to minimize the combined cost introduced by false positives (misidentify normal traffic as attack) and false negatives (misidentify attack traffic as normal) at any time. In this way, the adaptive defense system can generate fewer false alarms in normal situations or under light attacks with relaxed defense configurations, while protecting a network or a server more vigorously under severe attacks. In this paper, we present concrete adaptive defense system designs for defending against two major network attacks: SYN flood DDoS attack and Internet worm infection. The adaptive defense is a high-level system design that can be built on various underlying nonadaptive detection and filtering algorithms, which makes it applicable for a wide range of security defenses [J766]

"Complex Codebooks From Combinatorial Designs"

Codebooks (also called signal sets) meeting the Welch bounds are desirable in code-division multiple-access (CDMA) systems. In 2003, binary codebooks meeting Welch's bounds were constructed using difference sets by Ding, Golin, and Kloslashve. Recently, a generic construction of codebooks with cyclic difference sets meeting Welch's bound on the maximum cross-correlation amplitude was developed by Xia In this correspondence, the idea of Xia is extended, and related constructions of optimal codebooks with both cyclic and noncyclic difference sets are presented. These codebooks are optimal in the sense that they also meet this Welch bound. In addition, complex codebooks that almost meet Welch's bound on the maximum cross-correlation amplitude are also constructed with almost difference sets [J767]

"Freedom of silence vs. freedom of speech: Technology, law, and information security"

Freedom of speech and freedom of silence (privacy) are viewed very differently and are protected by laws in different ways in our society. In fact, there is a natural tension between the two, and society must find the proper balance between such opposing forces. Technology is playing an increasing role in supporting both freedom of speech and freedom of silence. At the same time, recent implications of freedom of silence on information security have become more and more apparent, as computer crimes are increasingly using unsolicited and often misleading speech, for example phishing emails and denial of service. This article explores the implications of the freedom of silence, and evaluates technological and legal solutions. The author concludes that technology-supported speech can more readily be contained by appropriate defending technologies than by legal means [J768]

"Attribute-Based Access Control with Hidden Policies and Hidden Credentials"

In an open environment such as the Internet, the decision to collaborate with a stranger (e.g., by granting access to a resource) is often based on the characteristics (rather than the identity) of the requester, via digital credentials: access is granted if Alice's credentials satisfy Bob's access policy. The literature contains many scenarios in which it is desirable to carry out such trust negotiations in a privacy-preserving manner, i.e., so as minimize the disclosure of credentials and/or of access policies. Elegant solutions were proposed for achieving various degrees of privacy-preservation through minimal disclosure. In this paper, we present protocols that protect both sensitive credentials and sensitive policies. That is, Alice gets the resource only if she satisfies the policy, Bob does not learn anything about Alice's credentials (not even whether Alice got access), and Alice learns neither Bob's policy structure nor which credentials caused her to gain access. Our protocols are efficient in terms of communication and in rounds of interaction [J769]

"A New Source Coding Scheme with Small Expected Length and Its Application to Simple Data Encryption"

We present a new source coding scheme with smaller expected length than Shannon-Fano-Elias codes. The ordering of source symbols input to the proposed encoding algorithm can be arbitrary. We show that this property leads to exponential complexity for eavesdropping even though an adversary knows the code construction rule and the probability mass function of the source [J770]

"On the Need for Signal-Coherent Watermarks"

Digital watermarking has been introduced in the 1990s as a complementary technology for copyright protection. In an effort to anticipate hostile behavior of adversaries, the research community is constantly introducing new attacks to benchmark watermarking systems. In this paper, we present a generic attack strategy based on block replacement. As multimedia content is often highly repetitive, the attack exploits signal's self-similarities to replace each signal block with another, perceptually similar one. Guided by the principles of the proposed attack framework, we implemented three attack algorithms for different types of multimedia content: video shots, audio

tracks and still images. Finally, considering the effectiveness of the proposed algorithms, we identify the properties that a watermark should have to counter this attacking strategy [J771]

"Iterative Source-Channel Decoding With Markov Random Field Source Models"

We propose a joint source-channel decoding approach for multidimensional correlated source signals. A Markov random field (MRF) source model is used which exemplarily considers the residual spatial correlations in an image signal after source encoding. Furthermore, the MRF parameters are selected via an analysis based on extrinsic information transfer charts. Due to the link between MRFs and the Gibbs distribution, the resulting soft-input soft-output (SISO) source decoder can be implemented with very low complexity. We prove that the inclusion of a high-rate block code after the quantization stage allows the MRF-based decoder to yield the maximum average extrinsic information. When channel codes are used for additional error protection the MRF-based SISO source decoder can be used as the outer constituent decoder in an iterative source-channel decoding scheme. Considering an example of a simple image transmission system we show that iterative decoding can be successfully employed for recovering the image data, especially when the channel is heavily corrupted [J772]

"Cybercrimes against Consumers: Could Biometric Technology Be the Solution?"

Although information technology's positive impacts on businesses and individuals are substantial, cybercrime continues to represent one of the greatest threats in the digital world. Advances in biometric technology's capabilities hold promise for solving this problem by offering users greater protection, but more legislative and social-policy work is needed to help realize the technology's full potential. In the near term, however, organizations can begin by incorporating users' security and privacy concerns into their biometric policies in terms of data collection, storage, access, and use [J773]

"An Adaptive Motion-Based Unequal Error Protection Approach for Real-Time Video Transport Over Wireless IP Networks"

In this work, we consider the delivery of digital video over future 3G wireless IP networks and we propose a low-complexity adaptive motion-based unequal error protection (UEP) video coding and transmission system which efficiently combines three existing error-resilience techniques by exploiting knowledge of the source material as well as the channel operating conditions. Given this information, the proposed system can adaptively adjust the operating parameters of the video source encoder and the forward error correction (FEC) channel encoder to maximize the delivered video quality based upon both application-layer video motion estimates and link-layer channel estimates. We demonstrate the efficacy of this approach using the ITU-T H.264 video source coder. The results indicate that a significant performance improvement can be achieved with enhanced resilience to inaccurate channel feedback information and with substantially reduced computational complexity compared to competing approaches [J774]

"On the design of bit-interleaved turbo-coded modulation with low error floors"

In this paper, we introduce an algorithm to optimize the performance in the error-floor region of bit-interleaved turbo-coded modulation (BITCM) on the additive white Gaussian noise channel. The key ingredient is an exact turbo code weight distribution algorithm producing a list of all codewords in the underlying turbo code of weight less than a given threshold. In BITCM, the information sequence is turbo-encoded, bit-interleaved, and mapped to signal points in a signal constellation. Using the union-bounding technique, we show that a well-designed bit interleaver is crucial to have a low error floor. Furthermore, the error-rate performance in the waterfall region depends on the bit interleaver, since the level of protection from channel noise on the bit level depends on the bit position and the neighboring bit values within the same symbol in the transmitted sequence. We observe a tradeoff between error-rate performance in the waterfall and error-floor regions, as illustrated by an extensive case study of a high-rate BITCM scheme. This tradeoff is typical in iterative decoding of turbo-like codes. The reported case study shows that it is possible to design bit interleavers with our proposed algorithm with equal or better performance in the waterfall region and superior performance in the error-floor region, compared with randomly generated bit interleavers. In particular, we were able to design BITCM schemes with maximum-likelihood decoding frame-error rates of 10-12and 10 -17at 2.6 and 3.8 dB away from unconstrained channel capacity, at spectral efficiencies of 3.10 and 6.20 b/s/Hz using square 16 and 256-quadrature amplitude modulation signal constellations, respectively [J775]

"Staying Protected from "Social Engineering""

"Your Internet Connection" we provided wealth of information on different protection tools. Although these tools

are indeed necessary for anyone brave enough to surf the Internet today, there is no substitute for sound judgement. "Your Internet Connection" describing Internet security resources, the Anti-Phishing Working Group's (APWG) and the Phishing Incident Reporting and Termination squad (http://wiki.castlecops.com/PIRT) were listed among other important security resources.Many criminals generating their garbage from the "sewers of the Internet" employ so called "social engineering" techniques. Just to make sure we are on the same page, here is the definition for the term "social engineering" from SearchSecurity.com: "In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. [J776]

СПИСОК ЛИТЕРАТУРЫ

J1. Ahmad S. Unequal Error Protection Using Fountain Codes With Applications to Video Communication. / Ahmad S., Hamzaoui R., Al-Akaidi M.M. // IEEE Transactions on Multimedia. - 2011. - Vol. 13, No. 1. - P. 92-101.

J2. Shouhuai Xu. Exploiting Trust-Based Social Networks for Distributed Protection of Sensitive Data. / Shouhuai Xu, Xiaohu Li, Parker T.P., Xueping Wang. // IEEE Transactions on Information Forensics and Security. - 2011. - Vol. 6, No. 1. - P. 39-52.

J3. Vaccaro A. An Integrated Framework for Smart Microgrids Modeling, Monitoring, Control, Communication, and Verification. / Vaccaro A., Popov M., Villacci D., Terzija V. // Proceedings of the IEEE. - 2011. - Vol. 99, No. 1. - P. 119-132.

J4. Sheng Li. Privacy Protection of Fingerprint Database. / Sheng Li, Kot A.C. // IEEE Signal Processing Letters. - 2011. - Vol. 18, No. 2. - P. 115-118.

J5. Rial A. A Privacy-Preserving Buyer-Seller Watermarking Protocol Based on Priced Oblivious Transfer. / Rial A., Balasch J., Preneel B. // IEEE Transactions on Information Forensics and Security. - 2011. - Vol. 6, No. 1. - P. 202-212.

J6. Ardagna C.A. An Obfuscation-Based Approach for Protecting Location Privacy. / Ardagna C.A., Cremonini M., De Capitani di Vimercati S., Samarati P. // IEEE Transactions on Dependable and Secure Computing. - 2011. - Vol. 8, No. 1. - P. 13-27.

J7. Kelkboom E.J.C. Preventing the Decodability Attack Based Cross-Matching in a Fuzzy Commitment Scheme. / Kelkboom E.J.C., Breebaart J., Kevenaar T.A.M., Buhan I., Veldhuis R.N.J. // IEEE Transactions on Information Forensics and Security. - 2011. - Vol. 6, No. 1. - P. 107-121.

J8. Nan Zhang. Privacy-Preserving OLAP: An Information-Theoretic Approach. / Nan Zhang, Wei Zhao. // IEEE Transactions on Knowledge and Data Engineering. - 2011. - Vol. 23, No. 1. - P. 122-138.

J9. Terzija V. Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks. / Terzija V., Valverde G., Deyu Cai, Regulski P., Madani V., Fitch J., Skok S., Begovic M.M., Phadke A. // Proceedings of the IEEE. - 2011. - Vol. 99, No. 1. - P. 80-93.

J10. Chowdhury K.R. OFDM-Based Common Control Channel Design for Cognitive Radio Ad Hoc Networks. / Chowdhury K.R., Akyldiz I.F. // IEEE Transactions on Mobile Computing. - 2011. - Vol. 10, No. 2. - P. 228-238.

J11. Ringelstein C. Papel: Provenance-Aware Policy Definition and Execution. / Ringelstein C., Staab S. // IEEE Internet Computing. - 2011. - Vol. 15, No. 1. - P. 49-58.

J12. Lei Bao. Iterative Encoder-Controller Design for Feedback Control Over Noisy Channels. / Lei Bao, Skoglund M., Johansson K.H. // IEEE Transactions on Automatic Control. - 2011. - Vol. 56, No. 2. - P. 265-278.

J13. Rudez U. Analysis of Underfrequency Load Shedding Using a Frequency Gradient. / Rudez U., Mihalic R. // IEEE Transactions on Power Delivery. - 2011. - Vol. 26, No. 2. - P. 565-575.

J14. Stefanovic. Urban Infrastructure-to-Vehicle Traffic Data Dissemination Using UEP Rateless Codes. / Stefanovic, C., Vukobratovic, D., Chiti F., Niccolai L., Crnojevic, V., Fantacci R. // IEEE Journal on Selected Areas in Communications. - 2011. - Vol. 29, No. 1. - P. 94-102.

J15. Esmaeili M.M. A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting. / Esmaeili M.M., Fatourechi M., Ward R.K. // IEEE Transactions on Information Forensics and Security. - 2011. - Vol. 6, No. 1. - P. 213-226.

J16. Xuhua Ding. Database Access Pattern Protection Without Full-Shuffles. / Xuhua Ding, Yanjiang Yang, Deng R.H. // IEEE Transactions on Information Forensics and Security. - 2011. - Vol. 6, No. 1. - P. 189-201.

J17. Heikkinen S. Service Usage Accounting. / Heikkinen S., Siltala S. // IEEE Vehicular Technology Magazine. - 2011. - Vol. 6, No. 1. - P. 60-67.

J18. Chowdhury Kaushik R. CRP: A Routing Protocol for Cognitive Radio Ad Hoc Networks. / Chowdhury Kaushik R., Akyildiz Ian F. // IEEE Journal on Selected Areas in Communications. - 2011. - Vol. 29, No. 4. - P. 794-804.

J19. Catalano D. Zero-Knowledge Sets With Short Proofs. / Catalano D., Di Raimondo M., Fiore D., Messina M. // IEEE Transactions on Information Theory. - 2011. - Vol. 57, No. 4. - P. 2488-2502.

J20. Schmidt A.U. Sender Scorecards. / Schmidt A.U., Leicher A., Shah Y., Cha I., Guccione L. // IEEE Vehicular Technology Magazine. - 2011. - Vol. 6, No. 1. - P. 52-59.

J21. Miyazaki T. Field Analysis of the Occurrence of Distribution-Line Faults Caused by Lightning Effects. / Miyazaki T., Okabe S. // IEEE Transactions on Electromagnetic Compatibility. - 2011. - Vol. 53, No. 1. - P. 114-121.

J22. Zhu L. Evidence theory-based fake measurement identification and fault-tolerant protection in digital substations. / Zhu L., Shi D., Duan X. // IET Generation, Transmission & Distribution. - 2011. - Vol. 5, No. 1. - P. 119-126.

J23. Kai Zheng. Scalable Pattern Matching on Multicore Platform via Dynamic Differentiated Distributed Detection (D). / Kai Zheng, Hongbin Lu, Nahum E. // IEEE Transactions on Computers. - 2011. - Vol. 60, No. 3. - P. 346-359.

J24. Doe Hyun Yoon. Virtualized ECC: Flexible Reliability in Main Memory. / Doe Hyun Yoon, Erez M. // IEEE Micro. - 2011. - Vol. 31, No. 1. - P. 11-19.

J25. Rosenfeld K. Attacks and Defenses for JTAG. / Rosenfeld K., Karri R. // IEEE Design & Test of Computers. - 2010. - Vol. 27, No. 1. - P. 36-47.

J26. Marin C. Robust MAC-lite and soft header recovery for packetized multimedia transmission. / Marin C., Leprovost Y., Kieffer M., Duhamel P. // IEEE Transactions on Communications. - 2010. - Vol. 58, No. 3. - P. 775-784.

J27. Battail G. Heredity as an Encoded Communication Process. IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 2. - P. 678-687.

J28. Upmanyu M. Blind Authentication: A Secure Crypto-Biometric Verification Protocol. / Upmanyu M., Namboodiri A.M., Srinathan K., Jawahar C.V. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 2. - P. 255-268.

J29. Siponen M. Compliance with Information Security Policies: An Empirical Investigation. / Siponen M., Pahnila S., Mahmood M.A. // Computer. - 2010. - Vol. 43, No. 2. - P. 64-71.

J30. Zhan J. Privacy-Preserving Collaborative Recommender Systems. / Zhan J., Chia-Lung Hsieh, I-Cheng Wang, Tsan-Sheng Hsu, Churn-Jung Liau, Da-Wei Wang. // IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews. - 2010. - Vol. 40, No. 4. - P. 472-476.

J31. Meng-Day Yu. Secure and Robust Error Correction for Physical Unclonable Functions. / Meng-Day Yu, Devadas S. // IEEE Design & Test of Computers. - 2010. - Vol. 27, No. 1. - P. 48-65.

J32. Nguyen H.X. Signal Transmission With Unequal Error Protection in Wireless Relay Networks. / Nguyen H.X., Nguyen H.H., Tho Le-Ngoc. // IEEE Transactions on Vehicular Technology. - 2010. - Vol. 59, No. 5. - P. 2166-2178.

J33. Phunchongharn P. A cognitive radio system for e-health applications in a hospital environment. / Phunchongharn P., Hossain E., Niyato D., Camorlinga S. // IEEE Wireless Communications. - 2010. - Vol. 17, No. 1. - P. 20-28.

J34. Ming Li. Data security and privacy in wireless body area networks. / Ming Li, Wenjing Lou, Kui Ren. // IEEE Wireless Communications. - 2010. - Vol. 17, No. 1. - P. 51-58.

J35. Tehranipoor Mohammad. Guest Editors' Introduction: Confronting the Hardware Trustworthiness Problem. / Tehranipoor Mohammad, Koushanfar Farinaz. // IEEE Design & Test of Computers. - 2010. - Vol. 27, No. 1. - P. 8-9.

J36. Kumar A. A New Framework for Adaptive Multimodal Biometrics Management. / Kumar A., Kanhangad V., Zhang D. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 1. - P. 92-102.

J37. David K. CAR-2-X and Pedestrian Safety. / David K., Flach A. // IEEE Vehicular Technology Magazine. - 2010. - Vol. 5, No. 1. - P. 70-76.

J38. Curone D. Heart Rate and Accelerometer Data Fusion for Activity Assessment of Rescuers During Emergency Interventions. / Curone D., Tognetti A., Secco E.L., Anania G., Carbonaro N., De Rossi D., Magenes G. // IEEE Transactions on Information Technology in Biomedicine. - 2010. - Vol. 14, No. 3. - P. 702-710.

J39. Gidel S. Pedestrian Detection and Tracking in an Urban Environment Using a Multilayer Laser Scanner. / Gidel S., Checchin P., Blanc C., Chateau T., Trassoudaine L. // IEEE Transactions on Intelligent Transportation Systems. - 2010. - Vol. 11, No. 3. - P. 579-588.

J40. Curone D. Smart Garments for Emergency Operators: The ProeTEX Project. / Curone D., Secco E.L., Tognetti A., Loriga G., Dudnik G., Risatti M., Whyte R., Bonfiglio A., Magenes G. // IEEE Transactions on Information Technology in Biomedicine. - 2010. - Vol. 14, No. 3. - P. 694-701.

J41. Krikidis I. Multilevel Modulation for Cognitive Multiaccess Relay Channel. IEEE Transactions on Vehicular Technology. - 2010. - Vol. 59, No. 6. - P. 3121-3125.

J42. Bose A. Smart Transmission Grid Applications and Their Supporting Infrastructure. IEEE Transactions on Smart Grid. - 2010. - Vol. 1, No. 1. - P. 11-19.

J43. Kotagiri S.P. Variations on Information Embedding in Multiple Access and Broadcast Channels. / Kotagiri S.P., Laneman J.N. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 5. - P. 2225-2240.

J44. Ruiqin Xiong. Optimal PET Protection for Streaming Scalably Compressed Video Streams With Limited Retransmission Based on Incomplete Feedback. / Ruiqin Xiong, Taubman D., Sivaraman V. // IEEE Transactions on Image Processing. - 2010. - Vol. 19, No. 9. - P. 2382-2395.

J45. Chin-Teng Lin. An Intelligent Telecardiology System Using a Wearable and Wireless ECG to Detect Atrial Fibrillation. / Chin-Teng Lin, Kuan-Cheng Chang, Chun-Ling Lin, Chia-Cheng Chiang, Shao-Wei Lu, Shih-Sheng Chang, Bor-Shyh Lin, Hsin-Yueh Liang, Ray-Jade Chen, Yuan-Teh Lee, Li-Wei Ko. // IEEE Transactions on Information Technology in Biomedicine. - 2010. - Vol. 14, No. 3. - P. 726-733.

J46. Clement A. PIPWatch Toolbar: Using Social Navigation to Enhance Privacy Protection and Compliance. / Clement A., Ley D., Costantino T., Kurtz D., Tissenbaum M. // IEEE Technology and Society Magazine. - 2010. - Vol. 29, No. 1. - P. 50-57.

J47. Ramachandran M. Path Computation Algorithms for Dynamic Service Provisioning With Protection and Inverse Multiplexing in SDH/SONET Networks. / Ramachandran M., Usha Rani N., Gonsalves T.A. // IEEE/ACM Transactions on Networking. - 2010. - Vol. 18, No. 5. - P. 1492-1504.

J48. Tiwari M. Gate-Level Information-Flow Tracking for Secure Architectures. / Tiwari M., Xun Li, Wassel H.M.G., Mazloom B., Mysore S., Chong F.T., Sherwood T. // IEEE Micro. - 2010. - Vol. 30, No. 1. - P. 92-100.

J49. Cassuto Y. Codes for Asymmetric Limited-Magnitude Errors With Application to Multilevel Flash Memories. / Cassuto Y., Schwartz M., Bohossian V., Bruck J. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 4. - P. 1582-1595.

J50. Alcaraz C. A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems. / Alcaraz C., Lopez J. // IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews. - 2010. - Vol. 40, No. 4. - P. 419-428.

J51. Cate F.H. The Limits of Notice and Choice. IEEE Security & Privacy. - 2010. - Vol. 8, No. 2. - P. 59-62.

J52. Potter Bruce. My Information, Your Code. IEEE Security & Privacy. - 2010. - Vol. 8, No. 2. - P. 51-53.

J53. Lanata A. Comparative Evaluation of Susceptibility to Motion Artifact in Different Wearable Systems for Monitoring Respiratory Rate. / Lanata A., Scilingo E.P., Nardini E., Loriga G., Paradiso R., De-Rossi D. // IEEE Transactions on Information Technology in Biomedicine. - 2010. - Vol. 14, No. 2. - P. 378-386.

J54. Xiaohong Quan. Hierarchical Segmentation of R&D Process and Intellectual Property Protection: Evidence From Multinational R&D Laboratories in China. / Xiaohong Quan, Chesbrough H. // IEEE Transactions on Engineering Management. - 2010. - Vol. 57, No. 1. - P. 9-21.

J55. Wenxin Guo. An Analytic Model-Based Approach for Power System Alarm Processing Employing Temporal Constraint Network. / Wenxin Guo, Fushuan Wen, Zhiwei Liao, Liuhong Wei, Jianbo Xin. // IEEE Transactions on Power Delivery. - 2010. - Vol. 25, No. 4. - P. 2435-2447.

J56. Chung-Hsuan Wang. On Unequal Error Protection of Convolutional Codes From an Algebraic Perspective. / Chung-Hsuan Wang, Mao-Ching Chiu, Chi-chao Chao. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 1. - P. 296-315.

J57. Feng Y.C. A Hybrid Approach for Generating Secure and Discriminating Face Template. / Feng Y.C., Yuen P.C., Jain A.K. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 1. - P. 103-117.

J58. Estrin D. Participatory sensing: applications and architecture [Internet Predictions]. IEEE Internet Computing. - 2010. - Vol. 14, No. 1. - P. 12-42.

J59. Cerf Vinton G. Internet predictions [Guest editor's introduction]. / Cerf Vinton G., Singh Munindar P. // IEEE Internet Computing. - 2010. - Vol. 14, No. 1. - P. 10-11.

J60. XiaoFeng Wang. Using Web-Referral Architectures to Mitigate Denial-of-Service Threats. / XiaoFeng Wang, Reiter M.K. // IEEE Transactions on Dependable and Secure Computing. - 2010. - Vol. 7, No. 2. - P. 203-216.

J61. Molch K. Multisensor and Multitemporal Fusion of VHR Satellite Imagery Based on KIM. IEEE Geoscience and Remote Sensing Letters. - 2010. - Vol. 7, No. 1. - P. 48-52.

J62. Gero. Survey of Pedestrian Detection for Advanced Driver Assistance Systems. / Gero,nimo D., Lo,pez A.M., Sappa A.D., Graf T. // IEEE Transactions on Pattern Analysis and Machine Intelligence. - 2010. - Vol. 32, No. 7. - P. 1239-1258.

J63. Lasko T.A. Spectral Anonymization of Data. / Lasko T.A., Vinterbo S.A. // IEEE Transactions on Knowledge and Data Engineering. - 2010. - Vol. 22, No. 3. - P. 437-446.

J64. Haodong Wang. Snoogle: A Search Engine for Pervasive Environments. / Haodong Wang, Tan C.C., Qun Li. // IEEE Transactions on Parallel and Distributed Systems. - 2010. - Vol. 21, No. 8. - P. 1188-1202.

J65. Tzu-Fang Sheu. In-Depth Packet Inspection Using a Hierarchical Pattern Matching Algorithm. / Tzu-Fang Sheu, Nen-Fu Huang, Hsiao-Ping Lee. // IEEE Transactions on Dependable and Secure Computing. - 2010. - Vol. 7, No. 2. - P. 175-188.

J66. Maggi F. Detecting Intrusions through System Call Sequence and Argument Analysis. / Maggi F., Matteucci M., Zanero S. // IEEE Transactions on Dependable and Secure Computing. - 2010. - Vol. 7, No. 4. - P. 381-395.

J67. Yanjiang Yang. Shifting Inference Control to User Side: Architecture and Protocol. / Yanjiang Yang, Yingjiu Li, Deng R.H., Feng Bao. // IEEE Transactions on Dependable and Secure Computing. - 2010. - Vol. 7, No. 2. - P. 189-202.

J68. Piva A. Secure Client-Side ST-DM Watermark Embedding. / Piva A., Bianchi T., De Rosa A. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 1. - P. 13-26.

J69. Bagchi-Sen S. Women in Cybersecurity: A Study of Career Advancement. / Bagchi-Sen S., Rao H.R., Upadhyaya S.J., Sangmi Chai. // IT Professional. - 2010. - Vol. 12, No. 1. - P. 24-31.

J70. Lisovich M.A. Inferring Personal Information from Demand-Response Systems. / Lisovich M.A., Mulligan D.K., Wicker S.B. // IEEE Security & Privacy. - 2010. - Vol. 8, No. 1. - P. 11-20.

J71. Rizomiliotis P. Message Origin Authentication and Integrity Protection in Chaos-Based Optical Communication. / Rizomiliotis P., Bogris A., Syvridis D. // IEEE Journal of Quantum Electronics. - 2010. - Vol. 46, No. 3. - P. 377-383.

J72. Chengshi Zhao. Joint sensing time and power allocation in cooperatively cognitive networks. / Chengshi Zhao, Kyungsup Kwak. // IEEE Communications Letters. - 2010. - Vol. 14, No. 2. - P. 163-165.

J73. Haibo Hu. 2PASS: Bandwidth-Optimized Location Cloaking for Anonymous Location-Based Services. / Haibo Hu, Jianliang Xu. // IEEE Transactions on Parallel and Distributed Systems. - 2010. - Vol. 21, No. 10. - P. 1458-1472.

J74. Valdes M.E. Method for Determining Selective Capability of Current-Limiting Overcurrent Devices Using Peak Let-Through Current-What Traditional Time-Current Curves Will Not Tell You. / Valdes M.E., Crabtree A.J., Papallo T. // IEEE Transactions on Industry Applications. - 2010. - Vol. 46, No. 2. - P. 603-611.

J75. Valdes M.E. Selectivity Analysis in Low-Voltage Power Distribution Systems With Fuses and Circuit Breakers. / Valdes M.E., Cline C., Hansen S., Papallo T. // IEEE Transactions on Industry Applications. - 2010. - Vol. 46, No. 2. - P. 593-602.

J76. Ozkaya A. R&D Team's Competencies, Innovation, and Growth With Knowledge Information Flow. IEEE Transactions on Engineering Management. - 2010. - Vol. 57, No. 3. - P. 416-429.

J77. Jing Zhang. Protecting Coherence and Entanglement by Quantum Feedback Controls. / Jing Zhang, Re-Bing Wu, Chun-Wen Li, Tzyh-Jong Tarn. // IEEE Transactions on Automatic Control. - 2010. - Vol. 55, No. 3. - P. 619-633.

J78. Yongjin Wang. An Analysis of Random Projection for Changeable and Privacy-Preserving Biometric Verification. / Yongjin Wang, Plataniotis K.N. // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. - 2010. - Vol. 40, No. 5. - P. 1280-1293.

J79. Rodrigues R.B. Lightning Data Observed With Lightning Location System in Portugal. / Rodrigues R.B., Mendes V.M.F., Catalao J.P.S. // IEEE Transactions on Power Delivery. - 2010. - Vol. 25, No. 2. - P. 870-875.

J80. Bernardos C.J. Advances in vehicular communications networks [Guest Editorial]. / Bernardos C.J., Festag A., Maxemchuk N.F., Pinart C., Weib C. // IEEE Network. - 2010. - Vol. 24, No. 1. - P. 4-5.

J81. {no data available}. Silver Bullet Security Podcast series. IEEE Transactions on Computers. - 2010. - Vol. 59, No. 3. - P. 432.

J82. Chun-I Fan. Anonymous Multireceiver Identity-Based Encryption. / Chun-I Fan, Ling-Ying Huang, Pei-Hsiu Ho. // IEEE Transactions on Computers. - 2010. - Vol. 59, No. 9. - P. 1239-1249.

J83. Dietzel S. Resilient secure aggregation for vehicular networks. / Dietzel S., Schoch E., Konings B., Weber M., Kargl F. // IEEE Network. - 2010. - Vol. 24, No. 1. - P. 26-31.

J84. Xiaohui Zhao. Steering Dynamic Collaborations Between Business Processes. / Xiaohui Zhao, Chengfei Liu. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2010. - Vol. 40, No. 4. - P. 743-757.

J85. Lingfei Jin. Application of Classical Hermitian Self-Orthogonal MDS Codes to Quantum MDS Codes. / Lingfei Jin, San Ling, Jinquan Luo, Chaoping Xing. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 9. - P. 4735-4740.

J86. Rial A. A Provably Secure Anonymous Buyer-Seller Watermarking Protocol. / Rial A., Mina Deng, Bianchi T., Piva A., Preneel B. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 4. - P. 920-931.

J87. Mills T.D. SCC18 Updates [Standards]. IEEE Industry Applications Magazine. - 2010. - Vol. 16, No. 5. - P. 74-77.

J88. Lili Guan. Joint Channel Estimation and PTS to Reduce Peak-to-Average-Power Radio in OFDM Systems Without Side Information. / Lili Guan, Tao Jiang, Daiming Qu, Yang Zhou. // IEEE Signal Processing Letters. - 2010. - Vol. 17, No. 10. - P. 883-886.

J89. Nan Li. Sharing location in online social networks. / Nan Li, Guanling Chen. // IEEE Network. - 2010. - Vol. 24, No. 5. - P. 20-25.

J90. Miskov-Zivanov N. Multiple Transient Faults in Combinational and Sequential Circuits: A Systematic Approach. / Miskov-Zivanov N., Marculescu D. // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. - 2010. - Vol. 29, No. 10. - P. 1614-1627.

J91. Nguyen H.X. Signal transmission with unequal error protection in relay selection networks. / Nguyen H.X., Nguyen H.H., Le-Ngoc T. // IET Communications. - 2010. - Vol. 4, No. 13. - P. 1624-1635.

J92. Ahmethodzic A. Design Improvement of a 245-kV Circuit Breaker With Double-Speed Mechanism Through Current Zero Analysis. / Ahmethodzic A., Smeets R.P.P., Kertesz V., Kapetanovic M., Sokolija K. // IEEE Transactions on Power Delivery. - 2010. - Vol. 25, No. 4. - P. 2496-2503.

J93. Stolfo Salvatore J. Privacy-Preserving Sharing of Sensitive Information. / Stolfo Salvatore J., Tsudik Gene. // IEEE Security & Privacy. - 2010. - Vol. 8, No. 4. - P. 16-17.

J94. Parise G. Level, Class, and Prospected Safety Performance of a Lightning Protection System for a Complex of Structures (LPCS). / Parise G., Martirano L., Lucheroni M. // IEEE Transactions on Industry Applications. - 2010. - Vol. 46, No. 5. - P. 2106-2110.

J95. Selkirk D. The Dangers of Grounding Resistor Failure. / Selkirk D., Savostianik M., Crawford K. // IEEE Industry Applications Magazine. - 2010. - Vol. 16, No. 5. - P. 53-58.

J96. Yi Zhang. Energy Efficiency in Telecom Optical Networks. / Yi Zhang, Chowdhury P., Tornatore M., Mukherjee B. // IEEE Communications Surveys & Tutorials. - 2010. - Vol. 12, No. 4. - P. 441-458.

J97. Georgakilas K.N. Performance Evaluation of Impairment-Aware Routing Under Single- and Double-Link Failures. / Georgakilas K.N., Katrinis K., Tzanakaki A., Madsen O.B. // IEEE/OSA Journal of Optical Communications and Networking. - 2010. - Vol. 2, No. 8. - P. 633-641.

J98. Blanch Juan. RAIM with Optimal Integrity and Continuity Allocations Under Multiple Failures. / Blanch Juan, Walter Todd, Enge Per. // IEEE Transactions on Aerospace and Electronic Systems. - 2010. - Vol. 46, No. 3. - P. 1235-1247.

J99. Hui Wan. An Adaptive Multiagent Approach to Protection Relay Coordination With Distributed Generators in Industrial Power Distribution System. / Hui Wan, Li K.K., Wong K.P. // IEEE Transactions on Industry Applications. - 2010. - Vol. 46, No. 5. - P. 2118-2124.

J100. Kshetri N. Cloud Computing in Developing Economies. Computer. - 2010. - Vol. 43, No. 10. - P. 47-55.

J101. Muc. Experimental Performance of Shared Path Protection With Flooded Versus Collected Sharing Resource Information in GMPLS WSON Networks. / Muc,oz R., Marti,nez R., Casellas R. // Journal of Lightwave Technology. - 2010. - Vol. 28, No. 23. - P. 3372-3386.

J102. Mugen Peng. McWiLL-A New Mobile Broadband Access Technology for Supporting Both Voice and Packet Services. / Mugen Peng, Guanghan Xu, Wenbo Wang, Hsiao-Hwa Chen. // IEEE Systems Journal. -

2010. - Vol. 4, No. 4. - P. 495-504.

J103. Krontiris I. Location privacy in urban sensing networks: research challenges and directions [Security and Privacy in Emerging Wireless Networks]. / Krontiris I., Freiling F.C., Dimitriou T. // IEEE Wireless Communications. - 2010. - Vol. 17, No. 5. - P. 30-35.

J104. Zhenning Kong. Resilience to Degree-Dependent and Cascading Node Failures in Random Geometric Networks. / Zhenning Kong, Yeh E.M. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 11. - P. 5533-5546.

J105. Yen C.-T. Digital product transaction mechanism for electronic auction environment. / Yen C.-T., Wu T.-C., Guo M.-H., Yang C.-K., Chao H.-C. // IET Information Security. - 2010. - Vol. 4, No. 4. - P. 248-257.

J106. Raji F. Anonymity and security for autonomous mobile agents. / Raji F., Ladani B.T. // IET Information Security. - 2010. - Vol. 4, No. 4. - P. 397-410.

J107. Simeone O. Robust Transmission and Interference Management For Femtocells with Unreliable Network Access. / Simeone O., Erkip E., Shamai Shitz S. // IEEE Journal on Selected Areas in Communications. - 2010. - Vol. 28, No. 9. - P. 1469-1478.

J108. Bishop S. Covert channel resistant information leakage protection using a multi-agent architecture. / Bishop S., Okhravi H., Rahimi S., Lee Y.-C. // IET Information Security. - 2010. - Vol. 4, No. 4. - P. 233-247.

J109. Hui-Yu Huang. A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation. / Hui-Yu Huang, Cheng-Han Yang, Wen-Hsing Hsu. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 4. - P. 625-637.

J110. Upendar J. PSO and ANN-based fault classification for protective relaying. / Upendar J., Gupta C.P., Singh G.K., Ramakrishna G. // IET Generation, Transmission & Distribution. - 2010. - Vol. 4, No. 10. - P. 1197-1212.

J111. Xunyu Pan. Region Duplication Detection Using Image Feature Matching. / Xunyu Pan, Siwei Lyu. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 4. - P. 857-867.

J112. Luna J. Data-Centric Privacy Protocol for Intensive Care Grids. / Luna J., Dikaiakos M., Marazakis M., Kyprianou T. // IEEE Transactions on Information Technology in Biomedicine. - 2010. - Vol. 14, No. 6. - P. 1327-1337.

J113. Cohen F. Automated Control System Security. IEEE Security & Privacy. - 2010. - Vol. 8, No. 5. - P. 62-63.

J114. Bruening P.J. Data Tagging for New Information Governance Models. / Bruening P.J., Waterman K.K. // IEEE Security & Privacy. - 2010. - Vol. 8, No. 5. - P. 64-68.

J115. Hui Jun Wu. Kernel Service Protection for Client Security. IEEE Security & Privacy. - 2010. - Vol. 8, No. 5. - P. 14-19.

J116. Abu-Nimeh S. Proliferation and Detection of Blog Spam. / Abu-Nimeh S., Chen T. // IEEE Security & Privacy. - 2010. - Vol. 8, No. 5. - P. 42-47.

J117. Xin Kang. Optimal power allocation for OFDM-based cognitive radio with new primary transmission protection criteria. / Xin Kang, Garg H., Ying-Chang Liang, Rui Zhang. // IEEE Transactions on Wireless Communications. - 2010. - Vol. 9, No. 6. - P. 2066-2075.

J118. Motahari S. Online Anonymity Protection in Computer-Mediated Communication. / Motahari S., Ziavras S.G., Jones Q. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 3. - P. 570-580.

J119. Rongxing Lu. An Intelligent Secure and Privacy-Preserving Parking Scheme Through Vehicular Communications. / Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xuemin Shen. // IEEE Transactions on Vehicular Technology. - 2010. - Vol. 59, No. 6. - P. 2772-2785.

J120. Qingke Wen. Classification of Grassland Types by MODIS Time-Series Images in Tibet, China. / Qingke

Wen, Zengxiang Zhang, Shuo Liu, Xiao Wang, Chen Wang. // IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing. - 2010. - Vol. 3, No. 3. - P. 404-409.

J121. Chun-Hsien Chou. A Perceptually Tuned Watermarking Scheme for Color Images. / Chun-Hsien Chou, Kuo-Cheng Liu. // IEEE Transactions on Image Processing. - 2010. - Vol. 19, No. 11. - P. 2966-2982.

J122. Fan-Zhi Kong. Electro-Thermo-Mechanical Characterizations of Various Wire Bonding Interconnects Illuminated by an Electromagnetic Pulse. / Fan-Zhi Kong, Wen-Yan Yin, Jun-Fa Mao, Qing Huo Liu. // IEEE Transactions on Advanced Packaging. - 2010. - Vol. 33, No. 3. - P. 729-737.

J123. Cerutti S. Guest Editorial Special Section on Smart Wearable Devices for Human Health and Protection. / Cerutti S., Magenes G., Bonato P. // IEEE Transactions on Information Technology in Biomedicine. - 2010. - Vol. 14, No. 3. - P. 691-693.

J124. Xiaoli Li. A Wavelet-PCA-Based Fingerprinting Scheme for Peer-to-Peer Video File Sharing. / Xiaoli Li, Krishnan S., Ngok-Wah Ma. // IEEE Transactions on Information Forensics and Security. - 2010. - Vol. 5, No. 3. - P. 365-373.

J125. Hobin Kim. Source-channel rate optimization for progressive image transmission over block fading relay channels [Transactions Papers]. / Hobin Kim, Annavajjala R., Cosman P., Milstein L. // IEEE Transactions on Communications. - 2010. - Vol. 58, No. 6. - P. 1631-1642.

J126. Bonatti P. A Rule-Based Trust Negotiation System. / Bonatti P., De Coi J.L., Olmedilla D., Sauro L. // IEEE Transactions on Knowledge and Data Engineering. - 2010. - Vol. 22, No. 11. - P. 1507-1520.

J127. Guilley S. Evaluation of Power Constant Dual-Rail Logics Countermeasures against DPA with Design Time Security Metrics. / Guilley S., Sauvage L., Flament F., Vinh-Nga Vong, Hoogvorst P., Pacalet R. // IEEE Transactions on Computers. - 2010. - Vol. 59, No. 9. - P. 1250-1263.

J128. Bahmani S. Joint Decoding of Unequally Protected JPEG2000 Bitstreams and Reed-Solomon Codes. / Bahmani S., Bajic I.V., HajShirmohammadi A. // IEEE Transactions on Image Processing. - 2010. - Vol. 19, No. 10. - P. 2693-2704.

J129. Zhengyou He. Improved Fault-Location System for Railway Distribution System Using Superimposed Signal. / Zhengyou He, Jun Zhang, Wei-hua Li, Xiangning Lin. // IEEE Transactions on Power Delivery. - 2010. - Vol. 25, No. 3. - P. 1899-1911.

J130. Tamo I. Correcting Limited-Magnitude Errors in the Rank-Modulation Scheme. / Tamo I., Schwartz M. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 6. - P. 2551-2560.

J131. Eckert S. Comparison of Automatic DSM Generation Modules by Processing IKONOS Stereo Data of an Urban Area. / Eckert S., Hollands T. // IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing. - 2010. - Vol. 3, No. 2. - P. 162-167.

J132. Miyazaki T. A Field Study of Lightning Surges Propagating Into Residences. / Miyazaki T., Ishii T., Okabe S. // IEEE Transactions on Electromagnetic Compatibility. - 2010. - Vol. 52, No. 4. - P. 921-928.

J133. Pinjia Zhang. A Transfer-Function-Based Thermal Model Reduction Study for Induction Machine Thermal Overload Protective Relays. / Pinjia Zhang, Yi Du, Habetler T.G. // IEEE Transactions on Industry Applications. - 2010. - Vol. 46, No. 5. - P. 1919-1926.

J134. Balasubramanian I. Impact of Available Fault Current Variations on Arc-Flash Calculations. / Balasubramanian I., Graham A.M. // IEEE Transactions on Industry Applications. - 2010. - Vol. 46, No. 5. - P. 1836-1842.

J135. Gangadharan G.R. Free/Open Services. / Gangadharan G.R., D'Andrea V., Weiss M. // IT Professional. - 2010. - Vol. 12, No. 6. - P. 24-30.

J136. Dong-Long Lin. Simulation and Measurements of Stray Minority Carrier Protection Structures in CMOS Image Sensors. / Dong-Long Lin, Ching-Chun Wang, Chia-Ling Wei. // IEEE Transactions on Electron Devices. - 2010. - Vol. 57, No. 9. - P. 2213-2220.

J137. Maguire J.R. Web-Application Security: From Reactive to Proactive. / Maguire J.R., Miller H.G. // IT Professional. - 2010. - Vol. 12, No. 4. - P. 7-9.

J138. Yelmo J.C. CITA03-Protection of Personal Information in User-centric Converged Service Platforms. / Yelmo J.C., Marti,nez C., del A,lamo J.M., Monjas M.A. // IEEE (Revista IEEE America Latina) Latin America Transactions. - 2010. - Vol. 8, No. 2. - P. 127-134.

J139. Xiangwei Zhou. Probabilistic Resource Allocation for Opportunistic Spectrum Access. / Xiangwei Zhou, Li G.Y., Dongdong Li, Dandan Wang, Soong A.C.K. // IEEE Transactions on Wireless Communications. - 2010. - Vol. 9, No. 9. - P. 2870-2879.

J140. Matsumoto S. Echonet: A Home Network Standard. IEEE Pervasive Computing. - 2010. - Vol. 9, No. 3. - P. 88-92.

J141. Velasco L. GMPLS-based Multidomain Restoration: Analysis, Strategies, Policies and Experimental Assessment. / Velasco L., Agraz F., Marti,nez R., Casellas R., Spadaro S., Muc,oz R., Junyent G. // IEEE/OSA Journal of Optical Communications and Networking. - 2010. - Vol. 2, No. 7. - P. 427-441.

J142. Ravikumar B. Comparison of Multiclass SVM Classification Methods to Use in a Supportive System for Distance Relay Coordination. / Ravikumar B., Thukaram D., Khincha H.P. // IEEE Transactions on Power Delivery. - 2010. - Vol. 25, No. 3. - P. 1296-1305.

J143. Manassero G. Fault-Location System for Multiterminal Transmission Lines. / Manassero G., Senger E.C., Nakagomi R.M., Pellini E.L., Rodrigues E.C.N. // IEEE Transactions on Power Delivery. - 2010. - Vol. 25, No. 3. - P. 1418-1426.

J144. Huan Xu. Robust Regression and Lasso. / Huan Xu, Caramanis C., Mannor S. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 7. - P. 3561-3574.

J145. Barg A. Codes in Permutations and Error Correction for Rank Modulation. / Barg A., Mazumdar A. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 7. - P. 3158-3165.

J146. Seferoglu H. Dynamic FEC Algorithms for TFRC Flows. / Seferoglu H., Markopoulou A., Kozat U.C., Civanlar M.R., Kempf J. // IEEE Transactions on Multimedia. - 2010. - Vol. 12, No. 8. - P. 869-885.

J147. Khisti A. Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. / Khisti A., Wornell G.W. // IEEE Transactions on Information Theory. - 2010. - Vol. 56, No. 7. - P. 3088-3104.

J148. Junghyun Nam. An off-line dictionary attack on a simple three-party key exchange protocol. / Junghyun Nam, Juryon Paik, Hyun-kyu Kang, Ung Kim, Dongho Won. // IEEE Communications Letters. - 2009. - Vol. 13, No. 3. - P. 205-207.

J149. Meeyoung Cha. Analyzing the Video Popularity Characteristics of Large-Scale User Generated Content Systems. / Meeyoung Cha, Haewoon Kwak, Rodriguez P., Yong-Yeol Ahn, Sue Moon. // IEEE/ACM Transactions on Networking. - 2009. - Vol. 17, No. 5. - P. 1357-1370.

J150. Cassuto Y. Cyclic Lowest Density MDS Array Codes. / Cassuto Y., Bruck J. // IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 4. - P. 1721-1729.

J151. Hogab Kang. MPEG-21 and Its Interoperability with Rights-Information Standards. / Hogab Kang, Keunyoung Lee, Taehyun Kim, Xin Wang. // IEEE Multimedia. - 2009. - Vol. 16, No. 1. - P. 94-99.

J152. Castelucio A. An AS-level overlay network for IP traceback. / Castelucio A., Ziviani A., Salles R. // IEEE Network. - 2009. - Vol. 23, No. 1. - P. 36-41.

J153. Yufei Tao. ANGEL: Enhancing the Utility of Generalization for Privacy Preserving Publication. / Yufei Tao, Hekang Chen, Xiaokui Xiao, Shuigeng Zhou, Donghui Zhang. // IEEE Transactions on Knowledge and Data Engineering. - 2009. - Vol. 21, No. 7. - P. 1073-1087.

J154. Zhenyu Wei. Spatio-Temporal Just Noticeable Distortion Profile for Grey Scale Image/Video in DCT Domain. / Zhenyu Wei, Ngan K.N. // IEEE Transactions on Circuits and Systems for Video Technology. - 2009. - Vol. 19, No. 3. - P. 337-346.

J155. Hsin-Yi Tsai. A Graph Approach to Quantitative Analysis of Control-Flow Obfuscating Transformations. / Hsin-Yi Tsai, Yu-Lun Huang, Wagner D. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 2. - P. 257-267.

J156. Kaza S. Topological Analysis of Criminal Activity Networks: Enhancing Transportation Security. / Kaza S., Xu J., Marshall B., Hsinchun Chen. // IEEE Transactions on Intelligent Transportation Systems. - 2009. - Vol. 10, No. 1. - P. 83-91.

J157. Lifeng Lai. Authentication Over Noisy Channels. / Lifeng Lai, El Gamal H., Poor H.V. // IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 2. - P. 906-916.

J158. Sankaran C.B. Network access security in next- generation 3GPP systems: A tutorial. IEEE Communications Magazine. - 2009. - Vol. 47, No. 2. - P. 84-91.

J159. Wahab A. Driving Profile Modeling and Recognition Based on Soft Computing Approach. / Wahab A., Chai Quek, Chin Keong Tan, Takeda K. // IEEE Transactions on Neural Networks. - 2009. - Vol. 20, No. 4. - P. 563-582.

J160. Miller J. One More Take on Identity. IEEE Internet Computing. - 2009. - Vol. 13, No. 2. - P. 99-101.

J161. Shuai Wang. On the Characterization and Optimization of On-Chip Cache Reliability against Soft Errors. / Shuai Wang, Jie Hu, Ziavras S.G. // IEEE Transactions on Computers. - 2009. - Vol. 58, No. 9. - P. 1171-1184.

J162. D'Antona G. State Estimation for the Localization of Harmonic Sources in Electric Distribution Systems. / D'Antona G., Muscas C., Sulis S. // IEEE Transactions on Instrumentation and Measurement. - 2009. - Vol. 58, No. 5. - P. 1462-1470.

J163. Bazelon C. Licensed or unlicensed: The economic considerations in incremental spectrum allocations. IEEE Communications Magazine. - 2009. - Vol. 47, No. 3. - P. 110-116.

J164. Laszlo M. Approximation Bounds for Minimum Information Loss Microaggregation. / Laszlo M., Mukherjee S. // IEEE Transactions on Knowledge and Data Engineering. - 2009. - Vol. 21, No. 11. - P. 1643-1647.

J165. Lei Zhang. A Modified Matched Filter With Double-Sided Thresholding for Screening Proliferative Diabetic Retinopathy. / Lei Zhang, Qin Li, You J., Zhang D. // IEEE Transactions on Information Technology in Biomedicine. - 2009. - Vol. 13, No. 4. - P. 528-534.

J166. Brouchier J. Temperature Attacks. / Brouchier J., Kean T., Marsh C., Naccache D. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 2. - P. 79-82.

J167. Nishimoto Y. Integrated Digital Rights Management for Mobile IPTV Using Broadcasting and Communications. / Nishimoto Y., Mita N., Imaizumi H. // IEEE Transactions on Broadcasting. - 2009. - Vol. 55, No. 2. - P. 419-424.

J168. Ananyi K. Flexible Hardware Processor for Elliptic Curve Cryptography Over NIST Prime Fields. / Ananyi K., Alrimeih H., Rakhmatov D. // IEEE Transactions on Very Large Scale Integration (VLSI) Systems. - 2009. - Vol. 17, No. 8. - P. 1099-1112.

J169. Aydinlik M. Performance Bounds for Unequal Error Protecting Turbo Codes. / Aydinlik M., Salehi M. // IEEE Transactions on Communications. - 2009. - Vol. 57, No. 5. - P. 1215-1220.

J170. Haiyun Xu. Fingerprint Verification Using Spectral Minutiae Representations. / Haiyun Xu, Veldhuis R.N.J., Bazen A.M., Kevenaar T.A.M., Akkermans T.A.H.M., Gokberk B. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 3. - P. 397-409.

J171. Jurca D. Forward Error Correction for Multipath Media Streaming. / Jurca D., Frossard P., Jovanovic A. // IEEE Transactions on Circuits and Systems for Video Technology. - 2009. - Vol. 19, No. 9. - P. 1315-1326.

J172. Nasruminallah. EXIT-Chart Optimized Short Block Codes for Iterative Joint Source and Channel Decoding in H.264 Video Telephony. / Nasruminallah, Hanzo L. // IEEE Transactions on Vehicular Technology. -

2009. - Vol. 58, No. 8. - P. 4306-4315.

J173. McGraw Gary. Silver Bullet Talks with Jeremiah Grossman. IEEE Security & Privacy. - 2009. - Vol. 7, No. 2. - P. 10-14.

J174. Guangyi Shi. Mobile Human Airbag System for Fall Protection Using MEMS Sensors and Embedded SVM Classifier. / Guangyi Shi, Cheung Shing Chan, Wen Jung Li, Kwok-Sui Leung, Yuexian Zou, Yufeng Jin. // IEEE Sensors Journal. - 2009. - Vol. 9, No. 5. - P. 495-503.

J175. Yu-Cheng Fan. De-Interlacing Algorithm Using Spatial-Temporal Correlation-Assisted Motion Estimation. / Yu-Cheng Fan, Chia-Hao Chung. // IEEE Transactions on Circuits and Systems for Video Technology. - 2009. - Vol. 19, No. 7. - P. 932-944.

J176. Manes G.W. Overview of Licensing and Legal Issues for Digital Forensic Investigators. / Manes G.W., Downing E. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 2. - P. 45-48.

J177. Harauz J. A New Era of Presidential Security: The President and His BlackBerry. / Harauz J., Kaufman L.M. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 2. - P. 67-70.

J178. Pfleeger Shari Lawrence. Searching for You (review of Googling Security: How Much Does Google Know About You? by G. Conti; 2008) [Book reviews]. IEEE Security & Privacy. - 2009. - Vol. 7, No. 2. - P. 15.

J179. Caloyannides M.A. Forensics Is So "Yesterday". IEEE Security & Privacy. - 2009. - Vol. 7, No. 2. - P. 18-25.

J180. Agarwal P. Robust Blind Watermarking of Point-Sampled Geometry. / Agarwal P., Prabhakaran B. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 1. - P. 36-48.

J181. Nergiz M.E. Multirelational k-Anonymity. / Nergiz M.E., Clifton C., Nergiz A.E. // IEEE Transactions on Knowledge and Data Engineering. - 2009. - Vol. 21, No. 8. - P. 1104-1117.

J182. Spiekermann S. Engineering Privacy. / Spiekermann S., Cranor L.F. // IEEE Transactions on Software Engineering. - 2009. - Vol. 35, No. 1. - P. 67-82.

J183. Vaidya J. Privacy-Preserving Kth Element Score over Vertically Partitioned Data. / Vaidya J., Clifton C.W. // IEEE Transactions on Knowledge and Data Engineering. - 2009. - Vol. 21, No. 2. - P. 253-258.

J184. Bretz K.J. Comparative Investigation of Tram Vibrations. / Bretz K.J., Kiraly T.L., Szuhay P., Moldovanyi T., Bretz K. // IEEE Transactions on Vehicular Technology. - 2009. - Vol. 58, No. 4. - P. 1640-1646.

J185. Hopper N. Provably Secure Steganography. / Hopper N., von Ahn L., Langford J. // IEEE Transactions on Computers. - 2009. - Vol. 58, No. 5. - P. 662-676.

J186. Groen J. Shadow Enhancement in Synthetic Aperture Sonar Using Fixed Focusing. / Groen J., Hansen R.E., Callow H.J., Sabel J.C., Sabo T.O. // IEEE Journal of Oceanic Engineering. - 2009. - Vol. 34, No. 3. - P. 269-284.

J187. Mirkovic J. Accurately Measuring Denial of Service in Simulation and Testbed Experiments. / Mirkovic J., Hussain A., Fahmy S., Reiher P., Thomas R.K. // IEEE Transactions on Dependable and Secure Computing. - 2009. - Vol. 6, No. 2. - P. 81-95.

J188. Vanegas C.A. Visualization of Simulated Urban Spaces: Inferring Parameterized Generation of Streets, Parcels, and Aerial Imagery. / Vanegas C.A., Aliaga D.G., Benes B., Waddell P. // IEEE Transactions on Visualization and Computer Graphics. - 2009. - Vol. 15, No. 3. - P. 424-435.

J189. Tague P. Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis. / Tague P., Slater D., Rogers J., Poovendran R. // IEEE Transactions on Dependable and Secure Computing. - 2009. - Vol. 6, No. 2. - P. 111-123.

J190. Chin-Fu Kuo. Dynamic Routing with Security Considerations. / Chin-Fu Kuo, Ai-Chun Pang, Sheng-Kun Chan. // IEEE Transactions on Parallel and Distributed Systems. - 2009. - Vol. 20, No. 1. - P. 48-58.

J191. Phan R.C.-W. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol—SASI. IEEE

Transactions on Dependable and Secure Computing. - 2009. - Vol. 6, No. 4. - P. 316-320.

J192. Mzrak A.T. Detecting Malicious Packet Losses. / Mzrak A.T., Savage S., Marzullo K. // IEEE Transactions on Parallel and Distributed Systems. - 2009. - Vol. 20, No. 2. - P. 191-206.

J193. Bo Rong. A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study. / Bo Rong, Hsiao-Hwa Chen, Yi Qian, Kejie Lu, Rose Qingyang Hu, Guizani S. // IEEE Transactions on Vehicular Technology. - 2009. - Vol. 58, No. 1. - P. 398-408.

J194. Gionis A. k-Anonymization with Minimal Loss of Information. / Gionis A., Tassa T. // IEEE Transactions on Knowledge and Data Engineering. - 2009. - Vol. 21, No. 2. - P. 206-219.

J195. Gao D. Beyond Output Voting: Detecting Compromised Replicas Using HMM-Based Behavioral Distance. / Gao D., Reiter M.K., Song D. // IEEE Transactions on Dependable and Secure Computing. - 2009. - Vol. 6, No. 2. - P. 96-110.

J196. Saidane A. The Design of a Generic Intrusion-Tolerant Architecture for Web Servers. / Saidane A., Nicomette V., Deswarte Y. // IEEE Transactions on Dependable and Secure Computing. - 2009. - Vol. 6, No. 1. - P. 45-58.

J197. Kvalbein A. Multiple Routing Configurations for Fast IP Network Recovery. / Kvalbein A., Hansen A.F., Cicic T., Gjessing S., Lysne O. // IEEE/ACM Transactions on Networking. - 2009. - Vol. 17, No. 2. - P. 473-486.

J198. Li K. Privacy-Aware Collaborative Spam Filtering. / Li K., Zhong Z., Ramaswamy L. // IEEE Transactions on Parallel and Distributed Systems. - 2009. - Vol. 20, No. 5. - P. 725-739.

J199. Taujuddin N.S.A. Secured MyVirtualPDA using advanced encryption standard. / Taujuddin N.S.A., Noor Z.M., Tukiran Z., Wahab M.H.A., Mutalib A.A. // IEEE Potentials. - 2009. - Vol. 28, No. 1. - P. 40-42.

J200. Hanson M.A. Body Area Sensor Networks: Challenges and Opportunities. / Hanson M.A., Powell H.C., Barth A.T., Ringgenberg K., Calhoun B.H., Aylor J.H., Lach J. // Computer. - 2009. - Vol. 42, No. 1. - P. 58-65.

J201. Burmester M. On the Security of Route Discovery in MANETs. / Burmester M., de Medeiros B. // IEEE Transactions on Mobile Computing. - 2009. - Vol. 8, No. 9. - P. 1180-1188.

J202. Kannavara R. Surveying secure processors. / Kannavara R., Bourbakis N.G. // IEEE Potentials. - 2009. - Vol. 28, No. 1. - P. 28-34.

J203. Kuhn R. Introducing "Insecure IT". / Kuhn R., Rossman H., Liu S. // IT Professional. - 2009. - Vol. 11, No. 1. - P. 24-26.

J204. Landau S. The NRC Takes on Data Mining, Behavioral Surveillance, and Privacy. IEEE Security & Privacy. - 2009. - Vol. 7, No. 1. - P. 58-62.

J205. Yuen-Yan Chan. Teaching for Conceptual Change in Security Awareness: A Case Study in Higher Education. / Yuen-Yan Chan, Wei V.K. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 1. - P. 68-71.

J206. {no data available}. Silver Bullet Security Podcast Series. IEEE Transactions on Mobile Computing. - 2009. - Vol. 8, No. 3. - P. 432.

J207. Plebani P. URBE: Web Service Retrieval Based on Similarity Evaluation. / Plebani P., Pernici B. // IEEE Transactions on Knowledge and Data Engineering. - 2009. - Vol. 21, No. 11. - P. 1629-1642.

J208. Eissa M.M. New principle for transmission line protection using phase portrait plane. IET Generation, Transmission & Distribution. - 2009. - Vol. 3, No. 1. - P. 49-56.

J209. Guruswami V. Better Binary List Decodable Codes Via Multilevel Concatenation. / Guruswami V., Rudra A. // IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 1. - P. 19-26.

J210. Xiangning Lin. Principles and Implementations of Hierarchical Region Defensive Systems of Power Grid. / Xiangning Lin, Zhengtian Li, Kecheng Wu, Hanli Weng. // IEEE Transactions on Power Delivery. - 2009. - Vol.

24, No. 1. - P. 30-37.

J211. Stockton D.P. Seed-oil-based coolants for transformers. / Stockton D.P., Bland J.R., McClanahan T., Wilson J., Harris D.L., McShane P. // IEEE Industry Applications Magazine. - 2009. - Vol. 15, No. 1. - P. 68-74.

J212. Borghetti A. Lightning-Induced Overvoltages Transferred Through Distribution Power Transformers. / Borghetti A., Morched A., Napolitano F., Nucci C.A., Paolone M. // IEEE Transactions on Power Delivery. - 2009. - Vol. 24, No. 1. - P. 360-372.

J213. Quazi T. Quality of service for multimedia traffic using cross-layer design. / Quazi T., Xu H.J., Takawira F. // IET Communications. - 2009. - Vol. 3, No. 1. - P. 83-90.

J214. Prouff E. Statistical Analysis of Second Order Differential Power Analysis. / Prouff E., Rivain M., Bevan R. // IEEE Transactions on Computers. - 2009. - Vol. 58, No. 6. - P. 799-811.

J215. Xiaoyang Tong. The Modeling and Verification of Peer-to-Peer Negotiating Multiagent Colored Petri Nets for Wide-Area Backup Protection. / Xiaoyang Tong, Xiaoru Wang, Hopkinson K.M. // IEEE Transactions on Power Delivery. - 2009. - Vol. 24, No. 1. - P. 61-72.

J216. {no data available}. Silver Bullet Security Podcast series. IEEE Transactions on Computers. - 2009. - Vol. 58, No. 2. - P. 288.

J217. Ozansoy C.R. The Application-View Model of the International Standard IEC 61850. / Ozansoy C.R., Zayegh A., Kalam A. // IEEE Transactions on Power Delivery. - 2009. - Vol. 24, No. 3. - P. 1132-1139.

J218. Rust A. Test-Driven Development for Spreadsheet Risk Management. / Rust A., McDaid K. // IEEE Software. - 2009. - Vol. 26, No. 5. - P. 31-36.

J219. Inhyok Cha. Trust in M2M communication. / Inhyok Cha, Shah Y., Schmidt A.U., Leicher A., Meyerstein M.V. // IEEE Vehicular Technology Magazine. - 2009. - Vol. 4, No. 3. - P. 69-75.

J220. Chou J.C.-Y. Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks. / Chou J.C.-Y., Lin B., Sen S., Spatscheck O. // IEEE/ACM Transactions on Networking. - 2009. - Vol. 17, No. 6. - P. 1711-1723.

J221. Kurosawa K. One-Wayness Equivalent to General Factoring. / Kurosawa K., Takagi T. // IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 9. - P. 4249-4262.

J222. Yan Dang. Knowledge sharing and diffusion patterns. / Yan Dang, Hsinchun Chen, Yulie Zhang, Roco M.C. // IEEE Nanotechnology Magazine. - 2009. - Vol. 3, No. 3. - P. 16-21.

J223. Sagiroglu S. Keyloggers. / Sagiroglu S., Canbek G. // IEEE Technology and Society Magazine. - 2009. - Vol. 28, No. 3. - P. 10-17.

J224. Pau L.-F. Privacy management service contacts as business opportunity. IEEE Technology and Society Magazine. - 2009. - Vol. 28, No. 3. - P. 55-63.

J225. Jian He. A Hybrid Conditions-Dependent Outage Model of a Transformer in Reliability Evaluation. / Jian He, Yuanzhang Sun, Peng Wang, Lin Cheng. // IEEE Transactions on Power Delivery. - 2009. - Vol. 24, No. 4. - P. 2025-2033.

J226. Chun-I Fan. Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics. / Chun-I Fan, Yi-Hui Lin. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 4. - P. 933-945.

J227. Rue R. Making the Best Use of Cybersecurity Economic Models. / Rue R., Pfleeger S.L. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 4. - P. 52-60.

J228. Hagen J. Human Relationships: A Never-Ending Security Education Challenge?. IEEE Security & Privacy. - 2009. - Vol. 7, No. 4. - P. 65-67.

J229. Hughes G.F. Disposal of Disk and Tape Data by Secure Sanitization. / Hughes G.F., Coughlin T.,

Commins D.M. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 4. - P. 29-34.

J230. Qun Ni. Privacy-Aware Role-Based Access Control. / Qun Ni, Bertino E., Lobo J., Calo S.B. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 4. - P. 35-43.

J231. Henning Ronda. Predictable Surprises. IEEE Security & Privacy. - 2009. - Vol. 7, No. 4. - P. 74-76.

J232. Levitin G. Redundancy vs. Protection in Defending Parallel Systems Against Unintentional and Intentional Impacts. / Levitin G., Hausken K. // IEEE Transactions on Reliability. - 2009. - Vol. 58, No. 4. - P. 679-690.

J233. Garny S. GEANT4 Transport Calculations for Neutrons and Photons Below 15 MeV. / Garny S., Leuthold G., Mares V., Paretzke H.G., Ruhm W. // IEEE Transactions on Nuclear Science. - 2009. - Vol. 56, No. 4. - P. 2392-2396.

J234. Krause A. Optimizing Sensing: From Water to the Web. / Krause A., Guestrin C. // Computer. - 2009. - Vol. 42, No. 8. - P. 38-45.

J235. Edwards C. Fighting the fakes [analysis]. Engineering & Technology. - 2009. - Vol. 4, No. 12. - P. 13.

J236. Liu S. Surviving Distributed Denial-of-Service Attacks. IT Professional. - 2009. - Vol. 11, No. 5. - P. 51-53.

J237. Sarkar T.K. Who Was James Clerk Maxwell and What Was and Is His Electromagnetic Theory?. / Sarkar T.K., Salazar-Palma M., Sengupta D.L. // IEEE Antennas and Propagation Magazine. - 2009. - Vol. 51, No. 4. - P. 97-116.

J238. Reibeling C. Positive train control for Australia. IEEE Vehicular Technology Magazine. - 2009. - Vol. 4, No. 4. - P. 35-44.

J239. Yonghyun Lee. Advanced Unloading Analysis Considering Lateral Velocity and Disk RPM Drop in Emergency Parking. / Yonghyun Lee, Ki-Hoon Kim, Seokhwan Kim, No-Cheol Park, Young-Pil Park, Kyoung-Su Park, Cheol-Soon Kim, Jingyoo Yoo. // IEEE Transactions on Magnetics. - 2009. - Vol. 45, No. 11. - P. 4937-4940.

J240. Borade S. Unequal Error Protection: An Information-Theoretic Perspective. / Borade S., Nakiboglu B., Lizhong Zheng. // IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 12. - P. 5511-5539.

J241. Ab-Rahman M.S. Transmission surveillance and self-restoration against fibre fault for time division multiplexing using passive optical network. / Ab-Rahman M.S., Ng B.C., Premadi A., Jumari K. // IET Communications. - 2009. - Vol. 3, No. 12. - P. 1896-1906.

J242. Creese S. Can Cognitive Science Help Us Make Online Risk More Tangible?. / Creese S., Lamberts K. // IEEE Intelligent Systems. - 2009. - Vol. 24, No. 6. - P. 32-36.

J243. Hennessy S. D. Data-centric security: Integrating data privacy and data security. / Hennessy S. D., Lauer G. D., Zunic N., Gerber B., Nelson A. C. // IBM Journal of Research and Development. - 2009. - Vol. 53, No. 2. - P. 2:1-2:12.

J244. de Sousa R.T. On the Vulnerabilities and Protections of the OLSR ad hoc Routing Protocol from the point of view of Trust. / de Sousa R.T., Adnane A.H., Bidan C., Me L. // IEEE (Revista IEEE America Latina) Latin America Transactions. - 2009. - Vol. 7, No. 5. - P. 594-602.

J245. Locasto M.E. Bickering In-Depth: Rethinking the Composition of Competing Security Systems. / Locasto M.E., Bratus S., Schulte B. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 6. - P. 77-81.

J246. Qi-Feng Liu. Time-Domain Investigation on Cable-Induced Transient Coupling Into Metallic Enclosures. / Qi-Feng Liu, Wen-Yan Yin, Min Tang, Pei Guo Liu, Jun-Fa Mao, Qing Huo Liu. // IEEE Transactions on Electromagnetic Compatibility. - 2009. - Vol. 51, No. 4. - P. 953-962.

J247. Vahlstrom W. Strategies for field testing medium voltage cables. IEEE Electrical Insulation Magazine. - 2009. - Vol. 25, No. 5. - P. 7-17.

J248. Lin W.S. Behavior Forensics With Side Information for Multimedia Fingerprinting Social Networks. / Lin

W.S., Zhao H.V., Liu K.J.R. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 4. - P. 911-927.

J249. Gardner R.W. Detecting Code Alteration by Creating a Temporary Memory Bottleneck. / Gardner R.W., Garera S., Rubin A.D. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 4. - P. 638-650.

J250. Osterweil E. Interadministrative Challenges in Managing DNSKEYs. / Osterweil E., Lixia Zhang. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 5. - P. 44-51.

J251. Bohli J.-M. Enhancing Electronic Voting Machines on the Example of Bingo Voting. / Bohli J.-M., Henrich C., Kempka C., Muller-Quade J., Rohrich S. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 4. - P. 745-750.

J252. Pasalic E. Probabilistic Versus Deterministic Algebraic Cryptanalysis-A Performance Comparison. IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 11. - P. 5233-5240.

J253. Cate F.H. Security, Privacy, and the Role of Law. IEEE Security & Privacy. - 2009. - Vol. 7, No. 5. - P. 60-63.

J254. Lesk M. Incentives to Innovate: Improve the Past or Break with It?. IEEE Security & Privacy. - 2009. - Vol. 7, No. 5. - P. 78-81.

J255. Donner Marc. New Models for Old. IEEE Security & Privacy. - 2009. - Vol. 7, No. 4. - P. 3-4.

J256. Cortada J.W. Think Piece: Preserving Records of the Past, Today. IEEE Annals of the History of Computing. - 2009. - Vol. 31, No. 2. - P. 88-87.

J257. Popov A. P. Biophysical mechanisms of modification of skin optical properties in the UV wavelength range with nanoparticles. / Popov A. P., Priezzhev A. V., Lademann J., Myllyla R. // Journal of Applied Physics. - 2009. - Vol. 105, No. 10. - P. 102035-102035-6.

J258. Macia-Fernandez G. Mathematical Model for Low-Rate DoS Attacks Against Application Servers. / Macia-Fernandez G., Diaz-Verdejo J.E., Garcia-Teodoro P. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 3. - P. 519-529.

J259. Serizawa Y. Verification of Distributed Real-Time Computer Network Architecture Associated With Off-The-Shelf and Dedicated Technologies. / Serizawa Y., Tanaka T., Yusa H., Koda Y., Yamashita G., Miyabe M., Katayama S., Tsuchiya T., Omata K. // IEEE Transactions on Power Delivery. - 2009. - Vol. 24, No. 3. - P. 1206-1217.

J260. Edwards C. Play the IT security game fun for all the enterprise!. Engineering & Technology. - 2009. - Vol. 4, No. 7. - P. 56-57.

J261. Lei Song. Accumulated-Downtime-Oriented Restoration Strategy With Service Differentiation in Survivable WDM Mesh Networks. / Lei Song, Mukherjee B. // IEEE/OSA Journal of Optical Communications and Networking. - 2009. - Vol. 1, No. 1. - P. 113-124.

J262. Brooks R.R. Automobile security concerns. / Brooks R.R., Sander S., Juan Deng, Taiber J. // IEEE Vehicular Technology Magazine. - 2009. - Vol. 4, No. 2. - P. 52-64.

J263. Metzner J.J. Simplification of Packet-Symbol Decoding With Errors, Deletions, Misordering of Packets, and No Sequence Numbers. IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 6. - P. 2626-2639.

J264. Pasalic E. On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers. IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 7. - P. 3398-3406.

J265. Islam K.M.Z. Linear diversity-embedding STBC: design issues and applications. / Islam K.M.Z., Rabiei P., Al-Dhahir N., Diggavi S.N., Calderbank A.R. // IEEE Transactions on Communications. - 2009. - Vol. 57, No. 6. - P. 1578-1583.

J266. Yangfan Zhong. Random-Coding Lower Bounds for the Error Exponent of Joint Quantization and

Watermarking Systems. / Yangfan Zhong, Alajaji F., Linder T. // IEEE Transactions on Information Theory. - 2009. - Vol. 55, No. 7. - P. 3264-3283.

J267. Lin W.S. Digital Image Source Coder Forensics Via Intrinsic Fingerprints. / Lin W.S., Tjoa S.K., Zhao H.V., Liu K. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 3. - P. 460-475.

J268. Sangmi Chai. Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. / Sangmi Chai, Bagchi-Sen S., Morrell C., Rao H.R., Upadhyaya S.J. // IEEE Transactions on Professional Communication. - 2009. - Vol. 52, No. 2. - P. 167-182.

J269. Uppal M. Compress-Forward Coding With BPSK Modulation for the Half-Duplex Gaussian Relay Channel. / Uppal M., Zhixin Liu, Stankovic V., Zixiang Xiong. // IEEE Transactions on Signal Processing. - 2009. - Vol. 57, No. 11. - P. 4467-4481.

J270. Xiangning Lin. Identification of Cross-Country Fault of Power Transformer for Fast Unblocking of Differential Protection. / Xiangning Lin, Hanli Weng, Bin Wang. // IEEE Transactions on Power Delivery. - 2009. - Vol. 24, No. 3. - P. 1079-1086.

J271. Miller H. Gilbert. Secure Cyberspace: Answering the Call for Intelligent Action. / Miller H. Gilbert, Murphy Richard H. // IT Professional. - 2009. - Vol. 11, No. 3. - P. 60-63.

J272. Toninelli A. Enabling secure service discovery in mobile healthcare enterprise networks. / Toninelli A., Montanari R., Corradi A. // IEEE Wireless Communications. - 2009. - Vol. 16, No. 3. - P. 24-32.

J273. Kiyavash N. Regular Simplex Fingerprints and Their Optimality Properties. / Kiyavash N., Moulin P., Kalker T. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 3. - P. 318-329.

J274. Larson D.K. When Sensitive IT Information Crosses Borders. / Larson D.K., Miller K.W. // IT Professional. - 2009. - Vol. 11, No. 4. - P. 56-59.

J275. Lopez G. A SWIFT Take on Identity Management. / Lopez G., Canovas O., Gomez-Skarmeta A.F., Girao J. // Computer. - 2009. - Vol. 42, No. 5. - P. 58-65.

J276. Hurlburt G.F. Privacy and/or Security: Take Your Pick. / Hurlburt G.F., Miller K.W., Voas J.M., Day J.M. // IT Professional. - 2009. - Vol. 11, No. 4. - P. 52-55.

J277. Bartoli A. The Reaction Time to Web Site Defacements. / Bartoli A., Davanzo G., Medvet E. // IEEE Internet Computing. - 2009. - Vol. 13, No. 4. - P. 52-58.

J278. Pavanello D. On the Current Peak Estimates Provided by Lightning Detection Networks for Lightning Return Strokes to Tall Towers. / Pavanello D., Rachidi F., Janischewskyj W., Rubinstein M., Shostak V.O., Nucci C.A., Cummins K.L., Hussein A.M., Jen-Shih Chang. // IEEE Transactions on Electromagnetic Compatibility. - 2009. - Vol. 51, No. 3. - P. 453-458.

J279. Tornatore M. Effects of Outdated Control Information in Control-Plane-Enabled Optical Networks With Path Protection. / Tornatore M., De Grandi F., Muoz R., Martinez R., Casellas R., Pattavina A. // IEEE/OSA Journal of Optical Communications and Networking. - 2009. - Vol. 1, No. 2. - P. A194-A204.

J280. Hosik Sohn. Content sharing between home networks by using personal information and associated fuzzy vault scheme. / Hosik Sohn, Yong Ro, Plataniotis K. // IEEE Transactions on Consumer Electronics. - 2009. - Vol. 55, No. 2. - P. 431-437.

J281. Hasan M.M. Online Partitioning for Scalable and Survivable Optical Networks. / Hasan M.M., Jue J.P. // IEEE/OSA Journal of Optical Communications and Networking. - 2009. - Vol. 1, No. 2. - P. A133-A142.

J282. Kia S.H. Diagnosis of Broken-Bar Fault in Induction Machines Using Discrete Wavelet Transform Without Slip Estimation. / Kia S.H., Henao H., Capolino G.-A. // IEEE Transactions on Industry Applications. - 2009. - Vol. 45, No. 4. - P. 1395-1404.

J283. Touzi R. Phase of Target Scattering for Wetland Characterization Using Polarimetric C-Band SAR. / Touzi R., Deschamps A., Rother G. // IEEE Transactions on Geoscience and Remote Sensing. - 2009. - Vol. 47, No. 9. - P. 3241-3261.

J284. Mai Vu. On the primary exclusive region of cognitive networks. / Mai Vu, Devroye N., Tarokh V. // IEEE Transactions on Wireless Communications. - 2009. - Vol. 8, No. 7. - P. 3380-3385.

J285. Bhaskar V. Performance of convolutional codes in asynchronous CDMA communications under imperfect phase-tracking conditions. / Bhaskar V., Joiner L.L. // IEEE Transactions on Communications. - 2009. - Vol. 57, No. 7. - P. 2052-2059.

J286. Pinjia Zhang. A DC Signal Injection-Based Thermal Protection Scheme for Soft-Starter-Connected Induction Motors. / Pinjia Zhang, Yi Du, Bin Lu, Habetler T.G. // IEEE Transactions on Industry Applications. - 2009. - Vol. 45, No. 4. - P. 1351-1358.

J287. Varna A.L. Fingerprinting Compressed Multimedia Signals. / Varna A.L., Shan He, Swaminathan A., Min Wu. // IEEE Transactions on Information Forensics and Security. - 2009. - Vol. 4, No. 3. - P. 330-345.

J288. Gaura E.I. Increasing Safety of Bomb Disposal Missions: A Body Sensor Network Approach. / Gaura E.I., Brusey J., Kemp J., Thake C.D. // IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews. - 2009. - Vol. 39, No. 6. - P. 621-636.

J289. {no data available}. Achievements in power [History]. IEEE Power and Energy Magazine. - 2009. - Vol. 7, No. 4. - P. 58-64.

J290. Johnson M.E. Security through Information Risk Management. / Johnson M.E., Goetz E., Pfleeger S.L. // IEEE Security & Privacy. - 2009. - Vol. 7, No. 3. - P. 45-52.

J291. Cereda P.R.M. Access Control Model Formalism using Adaptive Automaton. / Cereda P.R.M., Zorzo S.D. // IEEE (Revista IEEE America Latina) Latin America Transactions. - 2008. - Vol. 6, No. 5. - P. 443-452.

J292. Gasperi M.L. Method for AC Powerline Impedance Measurement. / Gasperi M.L., Jensen D.L., Rollay D.T. // IEEE Transactions on Industry Applications. - 2008. - Vol. 44, No. 4. - P. 1034-1037.

J293. Schaathun H.G. On the Assumption of Equal Contributions in Fingerprinting. IEEE Transactions on Information Forensics and Security. - 2008. - Vol. 3, No. 3. - P. 569-572.

J294. Lau V. Asymptotic tradeoff between cross-layer goodput gain and outage diversity in OFDMA systems with slow fading and delayed CSIT. / Lau V., Wing Kwan Ng, Hui D.S.W. // IEEE Transactions on Wireless Communications. - 2008. - Vol. 7, No. 7. - P. 2732-2739.

J295. Nawaz M. Sustainable land use using consensus mapping and conflict resolution. / Nawaz M., Sattar F. // IEEE Aerospace and Electronic Systems Magazine. - 2008. - Vol. 23, No. 7. - P. 32-38.

J296. {no data available}. Silver Bullet Security Podcast Series. IEEE Transactions on Computers. - 2008. - Vol. 57, No. 9. - P. 1295.

J297. Townend P. CROWN-C: A High-Assurance Service-Oriented Grid Middleware System. / Townend P., Jinpeng Huai, Jie Xu, Looker N., Dacheng Zhang, Jianxin Li, Liang Zhong. // Computer. - 2008. - Vol. 41, No. 8. - P. 30-38.

J298. Carin L. Cybersecurity Strategies: The QuERIES Methodology. / Carin L., Cybenko G., Hughes J. // Computer. - 2008. - Vol. 41, No. 8. - P. 20-26.

J299. Fritz S. A Conceptual Framework for Assessing the Benefits of a Global Earth Observation System of Systems. / Fritz S., Scholes R.J., Obersteiner M., Bouma J., Reyers B. // IEEE Systems Journal. - 2008. - Vol. 2, No. 3. - P. 338-348.

J300. Cheng-Han Lin. A RED-FEC Mechanism for Video Transmission Over WLANs. / Cheng-Han Lin, Ce-Kuen Shieh, Chilamkurti N.K., Chih-Heng Ke, Wen-Shyang Hwang. // IEEE Transactions on Broadcasting. - 2008. - Vol. 54, No. 3. - P. 517-524.

J301. Lei Guang. MAC layer misbehavior in wireless networks: challenges and solutions. / Lei Guang, Assi C., Benslimane A. // IEEE Wireless Communications. - 2008. - Vol. 15, No. 4. - P. 6-14.

J302. Fresia M. Determination of Optimal Distortion-Based Protection in Progressive Image Transmission: A

Heuristic Approach. / Fresia M., Lavagetto F. // IEEE Transactions on Image Processing. - 2008. - Vol. 17, No. 9. - P. 1654-1662.

J303. Youn Joo Lee. A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System. / Youn Joo Lee, Kang Ryoung Park, Sung Joo Lee, Kwanghyuk Bae, Jaihie Kim. // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. - 2008. - Vol. 38, No. 5. - P. 1302-1313.

J304. Davi M. Progress of the ITER equatorial vis/IR wide angle viewing system optical design. / Davi M., Corre Y., Guilhem D., Jullien F., Reichle R., Salasca S., Travere J. M., de la Cal E., Manzanares A., de Pablos J. L., Migozzi J. B. // Review of Scientific Instruments. - 2008. - Vol. 79, No. 10. - P. 10F509-10F509-3.

J305. Zimmer W. ArchiSafe: Legally Compliant Electronic Storage. / Zimmer W., Langkabel T., Hentrich C. // IT Professional. - 2008. - Vol. 10, No. 4. - P. 26-33.

J306. Heikkila F.M. E-Discovery: Identifying and Mitigating Security Risks during Litigation. IT Professional. - 2008. - Vol. 10, No. 4. - P. 20-25.

J307. Okabe S. Phenomena of leaking electromagnetic waves and high frequency surges from isolated joint of gas insulated switchgear. / Okabe S., Takami J., Nojima K. // IEEE Transactions on Dielectrics and Electrical Insulation. - 2008. - Vol. 15, No. 4. - P. 1006-1014.

J308. Celik M.U. Lookup-Table-Based Secure Client-Side Embedding for Spread-Spectrum Watermarks. / Celik M.U., Lemma A.N., Katzenbeisser S., van der Veen M. // IEEE Transactions on Information Forensics and Security. - 2008. - Vol. 3, No. 3. - P. 475-487.

J309. Pai S. Transactional Confidentiality in Sensor Networks. / Pai S., Bermudez S., Wicker S.B., Meingast M., Roosta T., Sastry S., Mulligan D.K. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 4. - P. 28-35.

J310. Bloch M. Wireless Information-Theoretic Security. / Bloch M., Barros J., Rodrigues M.R.D., McLaughlin S.W. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 6. - P. 2515-2534.

J311. Anthapadmanabhan N.P. On the Fingerprinting Capacity Under the Marking Assumption. / Anthapadmanabhan N.P., Barg A., Dumer I. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 6. - P. 2678-2689.

J312. Wilbanks L. Need to Share vs. Need to Assure. IT Professional. - 2008. - Vol. 10, No. 3. - P. 64.

J313. Wen-Shenq Juang. Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards. / Wen-Shenq Juang, Sian-Teng Chen, Horng-Twu Liaw. // IEEE Transactions on Industrial Electronics. - 2008. - Vol. 55, No. 6. - P. 2551-2556.

J314. Dusad S. Diversity Embedded Codes: Theory and Practice. / Dusad S., Diggavi S.N., Al-Dhahir N., Calderbank A.R. // IEEE Journal of Selected Topics in Signal Processing. - 2008. - Vol. 2, No. 2. - P. 202-219.

J315. Lesk M. Digital Rights Management and Individualized Pricing. IEEE Security & Privacy. - 2008. - Vol. 6, No. 3. - P. 76-79.

J316. Hawkey K. Searching for the Right Fit: Balancing IT Security Management Model Trade-Offs. / Hawkey K., Muldner K., Beznosov K. // IEEE Internet Computing. - 2008. - Vol. 12, No. 3. - P. 22-30.

J317. Churchill Elizabeth. Useful Computer Security. / Churchill Elizabeth, Nelson Les, Smetters Diana K. // IEEE Internet Computing. - 2008. - Vol. 12, No. 3. - P. 10-12.

J318. Heier S. Wind Power [a review of Grid Integration of Wind Energy Conversion Systems (S. Heier; 2006); book review]. IEEE Power and Energy Magazine. - 2008. - Vol. 6, No. 3. - P. 95-97.

J319. Buszta K. Challenges in Certification and Accreditation. IT Professional. - 2008. - Vol. 10, No. 3. - P. 56-59.

J320. Voas Jeffrey. Information and Quality Assurance: An Unsolved, Perpetual Problem for Past and Future Generations. / Voas Jeffrey, Wilbanks Linda. // IT Professional. - 2008. - Vol. 10, No. 3. - P. 10-13.

J321. Tapolcai J. A New Shared Segment Protection Method for Survivable Networks with Guaranteed Recovery Time. / Tapolcai J., Pin-Han Ho, Verchere D., Cinkler T., Haque A. // IEEE Transactions on Reliability. - 2008. - Vol. 57, No. 2. - P. 272-282.

J322. Dieu-Linh Truong. Recent progress in dynamic routing for shared protection in multidomain networks. / Dieu-Linh Truong, Jaumard B. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 6. - P. 112-119.

J323. {no data available}. IEEE-USA-Supported Genetic-information Nondiscrimination Act Signed into Law [IEEE-USA]. IEEE Antennas and Propagation Magazine. - 2008. - Vol. 50, No. 3. - P. 205.

J324. Eun-Ae Cho. Home gateway operating model using reference monitor for enhanced user comfort and privacy. / Eun-Ae Cho, Chang-Joo Moon, Doo-Kwon Baik. // IEEE Transactions on Consumer Electronics. - 2008. - Vol. 54, No. 2. - P. 494-500.

J325. Nian Liu. A Security Mechanism of Web Services-Based Communication for Wind Power Plants. / Nian Liu, Jianhua Zhang, Wenxia Liu. // IEEE Transactions on Power Delivery. - 2008. - Vol. 23, No. 4. - P. 1930-1938.

J326. Rabiei P. Differential diversity-embedding space-time block coding for 2 and 4 transmit antennas. / Rabiei P., Al-Dhahir N. // IEEE Transactions on Wireless Communications. - 2008. - Vol. 7, No. 7. - P. 2452-2457.

J327. Lamberger M. Analysis of the Hash Function Design Strategy Called SMASH. / Lamberger M., Pramstaller N., Rechberger C., Rijmen V. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 8. - P. 3647-3655.

J328. Kun Wang. SIISAM: A Model for Secure Inhomogeneous Information Systems. / Kun Wang, Zhonghai Yin, Lihua Zhou, Feng Yuan, Zengxin Li. // Computer. - 2008. - Vol. 41, No. 7. - P. 56-61.

J329. Torres V. Open DRM and the Future of Media. / Torres V., Serrao C., Dias M.S., Delgado J. // IEEE Multimedia. - 2008. - Vol. 15, No. 2. - P. 28-36.

J330. Lihua Weng. Error Exponent Regions for Gaussian Broadcast and Multiple-Access Channels. / Lihua Weng, Pradhan S.S., Anastasopoulos A. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 7. - P. 2919-2942.

J331. Yupu Hu. NTRUSign With a New Perturbation. / Yupu Hu, Baocang Wang, Wencai He. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 7. - P. 3216-3221.

J332. Kumar H. Security threats in wireless sensor networks. / Kumar H., Sarma D., Kar A. // IEEE Aerospace and Electronic Systems Magazine. - 2008. - Vol. 23, No. 6. - P. 39-45.

J333. Zeng Daniel Dajun. Guest Editors' Introduction: Special Section on Intelligence and Security Informatics. / Zeng Daniel Dajun, Chen Hsinchun, Wang Fei-Yue, Kargupta Hillol. // IEEE Transactions on Knowledge and Data Engineering. - 2008. - Vol. 20, No. 8. - P. 1009-1012.

J334. {no data available}. Silver Bullet Security Podcast Series. IEEE Transactions on Parallel and Distributed Systems. - 2008. - Vol. 19, No. 8. - P. 1152.

J335. Nitzkin J.L. Public health information infrastructure. / Nitzkin J.L., Buttery C. // IEEE Engineering in Medicine and Biology Magazine. - 2008. - Vol. 27, No. 6. - P. 16-20.

J336. Borenstein J. Privacy: A non-existent entity. IEEE Technology and Society Magazine. - 2008. - Vol. 27, No. 4. - P. 20-26.

J337. Paulson Linda Dailey. News Briefs. Computer. - 2008. - Vol. 41, No. 11. - P. 18-20.

J338. Dong-Hyuck Im. Vector Watermarking Robust to Both Global and Local Geometrical Distortions. / Dong-Hyuck Im, Hae-Yeoun Lee, Seung-Jin Ryu, Heung-Kyu Lee. // IEEE Signal Processing Letters. - 2008. - Vol. 15, {no data available}. - P. 789-792.

J339. Tekin E. The Gaussian Multiple Access Wire-Tap Channel. / Tekin E., Yener A. // IEEE Transactions on

Information Theory. - 2008. - Vol. 54, No. 12. - P. 5747-5755.

J340. Varma A.K. Improving Behavioral IO Buffer Modeling Based on IBIS. / Varma A.K., Steer M., Franzon P.D. // IEEE Transactions on Advanced Packaging. - 2008. - Vol. 31, No. 4. - P. 711-721.

J341. Chune Zhang. Multipurpose Watermarking Based on Multiscale Curvelet Transform. / Chune Zhang, Cheng L.L., Zhengding Qiu, Cheng L.M. // IEEE Transactions on Information Forensics and Security. - 2008. - Vol. 3, No. 4. - P. 611-619.

J342. Montagut F. Bridging Security and Fault Management within Distributed Workflow Management Systems. / Montagut F., Molva R. // IEEE Transactions on Services Computing. - 2008. - Vol. 1, No. 1. - P. 33-48.

J343. Ying Jian. A novel scheme for protecting receiver's location privacy in wireless sensor networks. / Ying Jian, Shigang Chen, Zhan Zhang, Liang Zhang. // IEEE Transactions on Wireless Communications. - 2008. - Vol. 7, No. 10. - P. 3769-3779.

J344. Okabe S. Evaluation of breakdown characteristics of gas insulated switchgears for non-standard lightning impulse waveforms under diverse conditions. / Okabe S., Yuasa S., Kaneko S., Ueta G. // IEEE Transactions on Dielectrics and Electrical Insulation. - 2008. - Vol. 15, No. 5. - P. 1415-1423.

J345. Katzenbeisser S. A Buyer-Seller Watermarking Protocol Based on Secure Embedding. / Katzenbeisser S., Lemma A., Celik M.U., van der Veen M., Maas M. // IEEE Transactions on Information Forensics and Security. - 2008. - Vol. 3, No. 4. - P. 783-786.

J346. Kai Wang. Hierarchical Watermarking of Semiregular Meshes Based on Wavelet Transform. / Kai Wang, Lavoue G., Denis F., Baskurt A. // IEEE Transactions on Information Forensics and Security. - 2008. - Vol. 3, No. 4. - P. 620-634.

J347. Tracy K. Identity management systems. IEEE Potentials. - 2008. - Vol. 27, No. 6. - P. 34-37.

J348. Miller K.W. Information Integrity and IT Professionals' Integrity, Intertwined. / Miller K.W., Voas J. // IT Professional. - 2008. - Vol. 10, No. 6. - P. 35-40.

J349. Miller Keith W. IT as a Profession: Is Competent Creation the Primary Goal?. / Miller Keith W., Voas Jeffrey. // IT Professional. - 2008. - Vol. 10, No. 6. - P. 15-17.

J350. Yau S.S. A Privacy Preserving Repository for Data Integration across Data Sharing Services. / Yau S.S., Yin Yin. // IEEE Transactions on Services Computing. - 2008. - Vol. 1, No. 3. - P. 130-140.

J351. Bessani A.N. The Crutial Way of Critical Infrastructure Protection. / Bessani A.N., Sousa P., Correia M., Neves N.F., Verissimo P. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 6. - P. 44-51.

J352. Parks R.C. Vulnerability Assessment for Critical Infrastructure Control Systems. / Parks R.C., Rogers E. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 6. - P. 37-43.

J353. Trellue Ron. Process Control System Security: Bootstrapping a Legacy. / Trellue Ron, Palmer Charles C. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 6. - P. 22-23.

J354. Hyejeong Lee. Secure user identification for consumer electronics devices. / Hyejeong Lee, Sang-Ho Lee, Taeseok Kim, Hyokyung Bahn. // IEEE Transactions on Consumer Electronics. - 2008. - Vol. 54, No. 4. - P. 1798-1802.

J355. Papadimitratos P. Secure vehicular communication systems: design and architecture. / Papadimitratos P., Buttyan L., Holczer T., Schoch E., Freudiger J., Raya M., Zhendong Ma, Kargl F., Kung A., Hubaux J.-P. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 11. - P. 100-109.

J356. Hallingstad G. Protected core networking: an architectural approach to secure and flexible communications. / Hallingstad G., Oudkerk S. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 11. - P. 35-41.

J357. Le Goff S.Y. A novel selected mapping technique for PAPR reduction in OFDM systems. / Le Goff S.Y., Boon Kien Khoo, Tsimenidis C.C., Sharif B.S. // IEEE Transactions on Communications. - 2008. - Vol. 56, No. 11. - P. 1775-1779.

J358. Dong-Su Kim. Multimodal biometric authentication using teeth image and voice in mobile environment. / Dong-Su Kim, Kwang-Seok Hong. // IEEE Transactions on Consumer Electronics. - 2008. - Vol. 54, No. 4. - P. 1790-1797.

J359. Jinpeng Wei. A Secure Information Flow Architecture for Web Service Platforms. / Jinpeng Wei, Singaravelu L., Pu C. // IEEE Transactions on Services Computing. - 2008. - Vol. 1, No. 2. - P. 75-87.

J360. Kargl F. Secure vehicular communication systems: implementation, performance, and research challenges. / Kargl F., Papadimitratos P., Buttyan L., Muter M., Schoch E., Wiedersheim B., Ta-Vinh Thong, Calandriello G., Held A., Kung A., Hubaux J.-P. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 11. - P. 110-118.

J361. Pagot E. Systematic Study of the Urban Postconflict Change Classification Performance Using Spectral and Structural Features in a Support Vector Machine. / Pagot E., Pesaresi M. // IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing. - 2008. - Vol. 1, No. 2. - P. 120-128.

J362. Chung-Hsuan Wang. Combined puncturing and path pruning for convolutional codes and the application to unequal error protection. / Chung-Hsuan Wang, Yi-Hsin Lin. // IEEE Transactions on Communications. - 2008. - Vol. 56, No. 9. - P. 1385-1389.

J363. Lawton G. New Technology Prevents Data Leakage. Computer. - 2008. - Vol. 41, No. 9. - P. 14-17.

J364. Pfleeger S.L. Choosing a Security Option: The InfoSecure Methodology. / Pfleeger S.L., Ciszek T. // IT Professional. - 2008. - Vol. 10, No. 5. - P. 46-52.

J365. {no data available}. Silver Bullet Security Podcast series. IEEE Transactions on Mobile Computing. - 2008. - Vol. 7, No. 11. - P. 1392.

J366. Gilany M. A New Strategy for Determining Fault Zones in Distance Relays. / Gilany M., Al-Kandari A., Madouh J. // IEEE Transactions on Power Delivery. - 2008. - Vol. 23, No. 4. - P. 1857-1863.

J367. Thorp J. Gaining a Wider Perspective. / Thorp J., Abur A., Begovic M., Giri J., Avila-Rosales R. // IEEE Power and Energy Magazine. - 2008. - Vol. 6, No. 5. - P. 43-51.

J368. {no data available}. Silver Bullet Security Podcast series. IEEE Transactions on Computers. - 2008. - Vol. 57, No. 10. - P. 1440.

J369. Pengcheng Zhu. Index Assignment for Quantized Beamforming MIMO Systems. / Pengcheng Zhu, Lan Tang, Yan Wang, Xiaohu You. // IEEE Transactions on Wireless Communications. - 2008. - Vol. 7, No. 8. - P. 2917-2922.

J370. Rane S. Systematic Lossy Error Protection of Video Signals. / Rane S., Baccichet P., Girod B. // IEEE Transactions on Circuits and Systems for Video Technology. - 2008. - Vol. 18, No. 10. - P. 1347-1360.

J371. {no data available}. Silver Bullet Security Podcasts. IEEE Transactions on Parallel and Distributed Systems. - 2008. - Vol. 19, No. 10. - P. 1439.

J372. Hernandez Martinez G. Design and simulation of a grounding grid for GIS substation. / Hernandez Martinez G., Venegas Rebollar V. // IEEE (Revista IEEE America Latina) Latin America Transactions. - 2008. - Vol. 6, No. 2. - P. 137-143.

J373. Higgs R.J. Nice Error Bases and Sylow Subgroups. IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 9. - P. 4199-4207.

J374. Chee-Wooi Ten. Vulnerability Assessment of Cybersecurity for SCADA Systems. / Chee-Wooi Ten, Chen-Ching Liu, Manimaran G. // IEEE Transactions on Power Systems. - 2008. - Vol. 23, No. 4. - P. 1836-1846.

J375. Chia-Chun Wu. A Secure Authentication Scheme with Anonymity for Wireless Communications. / Chia-Chun Wu, Wei-Bin Lee, Woei-Jiunn Tsaur. // IEEE Communications Letters. - 2008. - Vol. 12, No. 10. - P. 722-723.

J376. Trope R.L. Hardening the Target. / Trope R.L., Witt M., Adams W.J. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 5. - P. 77-81.

J377. Dusad S. Embedded Rank Distance Codes for ISI Channels. / Dusad S., Diggavi S.N., Calderbank A.R. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 11. - P. 4866-4886.

J378. Serpanos D.N. Security and Privacy in Distributed Smart Cameras. / Serpanos D.N., Papalambrou A. // Proceedings of the IEEE. - 2008. - Vol. 96, No. 10. - P. 1678-1687.

J379. Fleck S. Smart Camera Based Monitoring System and Its Application to Assisted Living. / Fleck S., Strasser W. // Proceedings of the IEEE. - 2008. - Vol. 96, No. 10. - P. 1698-1714.

J380. McLaughlin P. Cross-Border Data Flows and Increased Enforcement. IEEE Security & Privacy. - 2008. - Vol. 6, No. 5. - P. 58-61.

J381. Shiguo Lian. Digital rights management for the home TV based on scalable video coding. IEEE Transactions on Consumer Electronics. - 2008. - Vol. 54, No. 3. - P. 1287-1293.

J382. Hoffmann M. Spatial Partitioning in Self-Organizing Smart Camera Systems. / Hoffmann M., Wittke M., Hahner J., Muller-Schloer C. // IEEE Journal of Selected Topics in Signal Processing. - 2008. - Vol. 2, No. 4. - P. 480-492.

J383. Wilbanks L. When Black Hats Are Really White. IT Professional. - 2008. - Vol. 10, No. 5. - P. 64.

J384. Bishop M. Information Assurance Education: A Work In Progress. / Bishop M., Frincke D.A. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 5. - P. 54-57.

J385. Ryan J.J.C. Performance Metrics for Information Security Risk Management. / Ryan J.J.C., Ryan D.J. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 5. - P. 38-44.

J386. Wei Wang. Energy-Constrained Distortion Reduction Optimization for Wavelet-Based Coded Image Transmission in Wireless Sensor Networks. / Wei Wang, Dongming Peng, Honggang Wang, Sharif H., Hsiao-Hwa Chen. // IEEE Transactions on Multimedia. - 2008. - Vol. 10, No. 6. - P. 1169-1180.

J387. Golic J.D. Entropy Analysis and New Constructions of Biometric Key Generation Systems. / Golic J.D., Baltatu M. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 5. - P. 2026-2040.

J388. Shi Xiao. Tolerance of intentional attacks in complex communication networks. / Shi Xiao, Gaoxi Xiao, Tee Hiang Cheng. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 1. - P. 146-152.

J389. Tondel I.A. Security Requirements for the Rest of Us: A Survey. / Tondel I.A., Jaatun M.G., Meland P.H. // IEEE Software. - 2008. - Vol. 25, No. 1. - P. 20-27.

J390. Yung-Chih Tsai. Turbo Coded OFDM for Reducing PAPR and Error Rates. / Yung-Chih Tsai, Shang-Kang Deng, Kuan-Cheng Chen, Mao-Chao Lin. // IEEE Transactions on Wireless Communications. - 2008. - Vol. 7, No. 1. - P. 84-89.

J391. Samuel A. Context-Aware Adaptation of Access-Control Policies. / Samuel A., Ghafoor A., Bertino E. // IEEE Internet Computing. - 2008. - Vol. 12, No. 1. - P. 51-54.

J392. Chao Gong. A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking. / Chao Gong, Sarac K. // IEEE Transactions on Parallel and Distributed Systems. - 2008. - Vol. 19, No. 10. - P. 1310-1324.

J393. Jing-Ming Guo. Paired Subimage Matching Watermarking Method on Ordered Dither Images and Its High-Quality Progressive Coding. / Jing-Ming Guo, Soo-Chang Pei, Hua Lee. // IEEE Transactions on Multimedia. - 2008. - Vol. 10, No. 1. - P. 16-30.

J394. Merhav N. Optimal Watermark Embedding and Detection Strategies Under Limited Detection Resources. / Merhav N., Sabbag E. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 1. - P. 255-274.

J395. Diggavi S.N. Diversity Embedded Space-Time Codes. / Diggavi S.N., Calderbank A.R., Dusad S., Al-

Dhahir N. // IEEE Transactions on Information Theory. - 2008. - Vol. 54, No. 1. - P. 33-50.

J396. Jingxian Wu. Improved BDFE Using A Priori Information for Turbo Equalization. / Jingxian Wu, Sang-Yick Leong, Kah-Ping Lee, Chengshan Xiao, Olivier J.C. // IEEE Transactions on Wireless Communications. - 2008. - Vol. 7, No. 1. - P. 233-240.

J397. Cotsaces C. Face-Based Digital Signatures for Video Retrieval. / Cotsaces C., Nikolaidis N., Pitas I. // IEEE Transactions on Circuits and Systems for Video Technology. - 2008. - Vol. 18, No. 4. - P. 549-553.

J398. Campana O. An H.264/AVC Video Coder Based on a Multiple Description Scalar Quantizer. / Campana O., Contiero R., Mian G.A. // IEEE Transactions on Circuits and Systems for Video Technology. - 2008. - Vol. 18, No. 2. - P. 268-272.

J399. Xiao-Ping Zhang. A Novel Look-Up Table Design Method for Data Hiding With Reduced Distortion. / Xiao-Ping Zhang, Kan Li, Xiaofeng Wang. // IEEE Transactions on Circuits and Systems for Video Technology. - 2008. - Vol. 18, No. 6. - P. 769-776.

J400. Xiaoxin Wu. Anonymous Geo-Forwarding in MANETs through Location Cloaking. / Xiaoxin Wu, Jun Liu, Xiaoyan Hong, Bertino E. // IEEE Transactions on Parallel and Distributed Systems. - 2008. - Vol. 19, No. 10. - P. 1297-1309.

J401. Pearson S. Securing Information Transfer in Distributed Computing Environments. / Pearson S., Casassamont M., Novoa M. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 1. - P. 34-42.

J402. {no data available}. News Briefs. IT Professional. - 2008. - Vol. 10, No. 1. - P. 7-11.

J403. Naderi M.S. Modeling and detection of transformer internal incipient fault during impulse test. / Naderi M.S., Gharehpetian G.B., Abedi M., Blackburn T.R. // IEEE Transactions on Dielectrics and Electrical Insulation. - 2008. - Vol. 15, No. 1. - P. 284-291.

J404. Chakrabarti A. Grid Computing Security: A Taxonomy. / Chakrabarti A., Damodaran A., Sengupta S. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 1. - P. 44-51.

J405. Charalambous C.A. A Simulation Tool to Predict the Impact of Soil Topologies on Coupling Between a Light Rail System and Buried Third-Party Infrastructure. / Charalambous C.A., Cotton I., Aylott P. // IEEE Transactions on Vehicular Technology. - 2008. - Vol. 57, No. 3. - P. 1404-1416.

J406. Breaux T.D. Analyzing Regulatory Rules for Privacy and Security Requirements. / Breaux T.D., Anton A.I. // IEEE Transactions on Software Engineering. - 2008. - Vol. 34, No. 1. - P. 5-20.

J407. Vazquez E. Transformer Differential Protection Using Principal Component Analysis. / Vazquez E., Mijares I.I., Chacon O.L., Conde A. // IEEE Transactions on Power Delivery. - 2008. - Vol. 23, No. 1. - P. 67-72.

J408. Xuxian Jiang. Tracing Worm Break-In and Contaminations via Process Coloring: A Provenance-Preserving Approach. / Xuxian Jiang, Buchholz F., Walters A., Dongyan Xu, Yi-Min Wang, Spafford E.H. // IEEE Transactions on Parallel and Distributed Systems. - 2008. - Vol. 19, No. 7. - P. 890-902.

J409. Sengar H. Detecting VoIP Floods Using the Hellinger Distance. / Sengar H., Haining Wang, Wijesekera D., Jajodia S. // IEEE Transactions on Parallel and Distributed Systems. - 2008. - Vol. 19, No. 6. - P. 794-805.

J410. Wiszniewski A. Ultrasaturation Phenomenon in Power Transformers-Myths and Reality. / Wiszniewski A., Rebizant W., Bejmert D., Schiel L. // IEEE Transactions on Power Delivery. - 2008. - Vol. 23, No. 3. - P. 1327-1334.

J411. Kasztenny B. Modeling and Protection of Hexagonal Phase-Shifting Transformers-Part II: Protection. / Kasztenny B., Rosolowski E. // IEEE Transactions on Power Delivery. - 2008. - Vol. 23, No. 3. - P. 1351-1358.

J412. Jing Deng. Multipath Key Establishment for Wireless Sensor Networks Using Just-Enough Redundancy Transmission. / Jing Deng, Han Y.S. // IEEE Transactions on Dependable and Secure Computing. - 2008. - Vol. 5, No. 3. - P. 177-190.

J413. Fang Liu. SBK: A Self-Configuring Framework for Bootstrapping Keys in Sensor Networks. / Fang Liu, Xiuzhen Cheng, Liran Ma, Kai Xing. // IEEE Transactions on Mobile Computing. - 2008. - Vol. 7, No. 7. - P. 858-868.

J414. Tapolcai J. TROP: A Novel Approximate Link-State Dissemination Framework For Dynamic Survivable Routing in MPLS Networks. / Tapolcai J., Pin-Han Ho, Haque A. // IEEE Transactions on Parallel and Distributed Systems. - 2008. - Vol. 19, No. 3. - P. 311-322.

J415. Kundur D. Security and Privacy for Distributed Multimedia Sensor Networks. / Kundur D., Luh W., Okorafor U.N., Zourntos T. // Proceedings of the IEEE. - 2008. - Vol. 96, No. 1. - P. 112-130.

J416. Wei-Bin Lee. A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations. / Wei-Bin Lee, Chien-Ding Lee. // IEEE Transactions on Information Technology in Biomedicine. - 2008. - Vol. 12, No. 1. - P. 34-41.

J417. Hung-Ta Pai. Power-Efficient Direct-Voting Assurance for Data Fusion in Wireless Sensor Networks. / Hung-Ta Pai, Han Y.S. // IEEE Transactions on Computers. - 2008. - Vol. 57, No. 2. - P. 261-273.

J418. Zhenhai Duan. Controlling IP Spoofing through Interdomain Packet Filters. / Zhenhai Duan, Xin Yuan, Chandrashekar J. // IEEE Transactions on Dependable and Secure Computing. - 2008. - Vol. 5, No. 1. - P. 22-36.

J419. Sebe F. Efficient Remote Data Possession Checking in Critical Information Infrastructures. / Sebe F., Domingo-Ferrer J., Martinez-Balleste A., Deswarte Y., Quisquater J.-J. // IEEE Transactions on Knowledge and Data Engineering. - 2008. - Vol. 20, No. 8. - P. 1034-1038.

J420. Gedik B. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. / Gedik B., Ling Liu. // IEEE Transactions on Mobile Computing. - 2008. - Vol. 7, No. 1. - P. 1-18.

J421. Nan Zhang. Privacy Protection Against Malicious Adversaries in Distributed Information Sharing Systems. / Nan Zhang, Wei Zhao. // IEEE Transactions on Knowledge and Data Engineering. - 2008. - Vol. 20, No. 8. - P. 1028-1033.

J422. Yu Chen. Protection of Database Security via Collaborative Inference Detection. / Yu Chen, Chu W.W. // IEEE Transactions on Knowledge and Data Engineering. - 2008. - Vol. 20, No. 8. - P. 1013-1027.

J423. Mirkovic J. Testing a Collaborative DDoS Defense In a Red Team/Blue Team Exercise. / Mirkovic J., Reiher P., Papadopoulos C., Hussain A., Shepard M., Berg M., Jung R. // IEEE Transactions on Computers. - 2008. - Vol. 57, No. 8. - P. 1098-1112.

J424. Kahn S. Medical Record Privacy and Security in a Digital Environment. / Kahn S., Sheshadri V. // IT Professional. - 2008. - Vol. 10, No. 2. - P. 46-52.

J425. Claveirole T. Securing wireless sensor networks against aggregator compromises. / Claveirole T., de Amorim M.D., Abdalla M., Viniotis Y. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 4. - P. 134-141.

J426. Nait-Abdesselam F. Detecting and avoiding wormhole attacks in wireless ad hoc networks. IEEE Communications Magazine. - 2008. - Vol. 46, No. 4. - P. 127-133.

J427. Moller J.E. Experiences with Electronic Health Records. / Moller J.E., Vosegaard H. // IT Professional. - 2008. - Vol. 10, No. 2. - P. 19-23.

J428. Varshney L.R. Local fidelity, constrained codes, and the Meru Prastara. IEEE Potentials. - 2008. - Vol. 27, No. 2. - P. 27-32.

J429. Yunjun Xu. Chattering Free Robust Control for Nonlinear Systems. IEEE Transactions on Control Systems Technology. - 2008. - Vol. 16, No. 6. - P. 1352-1359.

J430. Rose S. Minimizing information leakage in the DNS. / Rose S., Nakassis A. // IEEE Network. - 2008. - Vol. 22, No. 2. - P. 22-25.

J431. Jong Hwan Park. Public Key Broadcast Encryption Schemes With Shorter Transmissions. / Jong Hwan

Park, Hee Jean Kim, Sung M.H., Dong Hoon Lee. // IEEE Transactions on Broadcasting. - 2008. - Vol. 54, No. 3. - P. 401-411.

J432. Okabe S. Evaluation of Breakdown Characteristics of Gas Insulated Switchgears for Non-Standard Lightning Impulse Waveforms-Breakdown Characteristics for Non-Standard Lightning Impulse Waveforms Associated with Lightning Surges. / Okabe S., Yuasa S., Kaneko S. // IEEE Transactions on Dielectrics and Electrical Insulation. - 2008. - Vol. 15, No. 2. - P. 407-415.

J433. Acquisti A. Identity Management, Privacy, and Price Discrimination. IEEE Security & Privacy. - 2008. - Vol. 6, No. 2. - P. 46-50.

J434. Hansen M. Privacy and Identity Management. / Hansen M., Schwartz A., Cooper A. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 2. - P. 38-45.

J435. Wasserkrug S. Inference of Security Hazards from Event Composition Based on Incomplete or Uncertain Information. / Wasserkrug S., Gal A., Etzion O. // IEEE Transactions on Knowledge and Data Engineering. - 2008. - Vol. 20, No. 8. - P. 1111-1114.

J436. Locasto M.E. The Hidden Difficulties of Watching and Rebuilding Networks. / Locasto M.E., Stavrou A. // IEEE Security & Privacy. - 2008. - Vol. 6, No. 2. - P. 79-82.

J437. Garfinkel Simson. Sharp Figures, Fuzzy Purpose. IEEE Security & Privacy. - 2008. - Vol. 6, No. 2. - P. 5.

J438. Choudhury T. The Mobile Sensing Platform: An Embedded Activity Recognition System. / Choudhury T., Consolvo S., Harrison B., Hightower J., LaMarca A., LeGrand L., Rahimi A., Rea A., Bordello G., Hemingway B., Klasnja P., Koscher K., Landay J.A., Lester J., Wyatt D., Haehnel D. // IEEE Pervasive Computing. - 2008. - Vol. 7, No. 2. - P. 32-41.

J439. Law C.T. Fiber-Optics-Based Fault Detection in Power Systems. / Law C.T., Bhattarai K., Yu D.C. // IEEE Transactions on Power Delivery. - 2008. - Vol. 23, No. 3. - P. 1271-1279.

J440. Villa O. Accelerating Real-Time String Searching with Multicore Processors. / Villa O., Scarpazza D.P., Petrini F. // Computer. - 2008. - Vol. 41, No. 4. - P. 42-50.

J441. Cardoso G. Identifying the Primary Fault Section After Contingencies in Bulk Power Systems. / Cardoso G., Rolim J.G., Zurn H.H. // IEEE Transactions on Power Delivery. - 2008. - Vol. 23, No. 3. - P. 1335-1342.

J442. Niemiec M. Reviews of [("Security for Mobile Networks and Platforms", Aissi, S., et al) and (Cooperation in Wireless Networks: Principles and Applications, Fitzek, H.P. and Katz, M.D., Eds.; 2006)]. / Niemiec M., Szott S. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 3. - P. 20-22.

J443. Pereira F. Multimedia Retrieval and Delivery: Essential Metadata Challenges and Standards. / Pereira F., Vetro A., Sikora T. // Proceedings of the IEEE. - 2008. - Vol. 96, No. 4. - P. 721-744.

J444. Miller Jim. Is Anybody Home?. IEEE Internet Computing. - 2008. - Vol. 12, No. 2. - P. 91-93.

J445. Bhatia R.S. Bandwidth Guaranteed Routing With Fast Restoration Against Link and Node Failures. / Bhatia R.S., Kodialam M., Lakshman T.V., Sengupta S. // IEEE/ACM Transactions on Networking. - 2008. - Vol. 16, No. 6. - P. 1321-1330.

J446. Sartipi M. Distributed source coding using short to moderate length rate-compatible LDPC codes: the entire Slepian-Wolf rate region. / Sartipi M., Fekri F. // IEEE Transactions on Communications. - 2008. - Vol. 56, No. 3. - P. 400-411.

J447. Mihcak M.K. On Minimax Optimal Linear Transforms for Detection with Side Information in Gaussian Setup. / Mihcak M.K., Altug Y., Ayerden N.P. // IEEE Communications Letters. - 2008. - Vol. 12, No. 3. - P. 164-166.

J448. Caimu Tang. Mobile Privacy in Wireless Networks-Revisited. / Caimu Tang, Wu D.O. // IEEE Transactions on Wireless Communications. - 2008. - Vol. 7, No. 3. - P. 1035-1042.

J449. Dongmei Wang. Efficient Distributed Bandwidth Management for MPLS Fast Reroute. / Dongmei Wang,

Guangzhi Li. // IEEE/ACM Transactions on Networking. - 2008. - Vol. 16, No. 2. - P. 486-495.

J450. Venkitasubramaniam P. Toward an analytical approach to anonymous wireless networking. / Venkitasubramaniam P., Ting He, Lang Tong, Wicker S.B., University C. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 2. - P. 140-146.

J451. Ki-Woong Park. Computationally Efficient PKI-Based Single Sign-On Protocol, PKASSO for Mobile Devices. / Ki-Woong Park, Sang Seok Lim, Kyu Ho Park. // IEEE Transactions on Computers. - 2008. - Vol. 57, No. 6. - P. 821-834.

J452. Samantaray S.R. High impedance fault detection in power distribution networks using time-frequency transform and probabilistic neural network. / Samantaray S.R., Panigrahi B.K., Dash P.K. // IET Generation, Transmission & Distribution. - 2008. - Vol. 2, No. 2. - P. 261-270.

J453. Nikolaidis V.C. Design Strategies for Load-Shedding Schemes Against Voltage Collapse in the Hellenic System. / Nikolaidis V.C., Vournas C.D. // IEEE Transactions on Power Systems. - 2008. - Vol. 23, No. 2. - P. 582-591.

J454. Biswas G.P. Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key. IET Information Security. - 2008. - Vol. 2, No. 1. - P. 12-18.

J455. Hecker M. Privacy Ontology Support for E-Commerce. / Hecker M., Dillon T.S., Chang E. // IEEE Internet Computing. - 2008. - Vol. 12, No. 2. - P. 54-61.

J456. Yan Sun. Defense of trust management vulnerabilities in distributed networks. / Yan Sun, Zhu Han, Liu K.J.R. // IEEE Communications Magazine. - 2008. - Vol. 46, No. 2. - P. 112-119.

J457. Somekh-Baruch A. Achievable Error Exponents for the Private Fingerprinting Game. / Somekh-Baruch A., Merhav N. // IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 5. - P. 1827-1838.

J458. Yue G. Analysis and Design of Finite-Length LDPC Codes. / Yue G., Lu B., Wang X. // IEEE Transactions on Vehicular Technology. - 2007. - Vol. 56, No. 3. - P. 1321-1332.

J459. C. Jin. Web dual watermarking technology using an XML document. / C. Jin, Z.-G. Qu, Z.-M. Zhang, Y. Jiang. // IET Information Security. - 2007. - Vol. 1, No. 1. - P. 37-42.

J460. Reay I.K. A Survey and Analysis of the P3P Protocol's Agents, Adoption, Maintenance, and Future. / Reay I.K., Beatty P., Dick S., Miller J. // IEEE Transactions on Dependable and Secure Computing. - 2007. - Vol. 4, No. 2. - P. 151-164.

J461. Liggett D. Training and qualifying your employees. IEEE Industry Applications Magazine. - 2007. - Vol. 13, No. 3. - P. 25-30.

J462. Dantu R. Fast Worm Containment Using Feedback Control. / Dantu R., Cangussu J.W., Patwardhan S. // IEEE Transactions on Dependable and Secure Computing. - 2007. - Vol. 4, No. 2. - P. 119-136.

J463. Norman B.C. Virtual perimeter security (VPS) in a physical protection system. / Norman B.C., Adams D.G. // IEEE Aerospace and Electronic Systems Magazine. - 2007. - Vol. 22, No. 4. - P. 30-33.

J464. Liebrock L.M. Scholarship for Service: New Mexico Tech's Undergraduate Program. IEEE Distributed Systems Online. - 2007. - Vol. 8, No. 3. - P. 2.

J465. Zhang N. Privacy-Preserving Data Mining Systems. / Zhang N., Zhao W. // Computer. - 2007. - Vol. 40, No. 4. - P. 52-58.

J466. Chen R. A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks. / Chen R., Park J.-M., Marchany R. // IEEE Transactions on Parallel and Distributed Systems. - 2007. - Vol. 18, No. 5. - P. 577-588.

J467. Potlapally N.R. Aiding Side-Channel Attacks on Cryptographic Software With Satisfiability-Based Analysis. / Potlapally N.R., Raghunathan A., Ravi S., Jha N.K., Lee R.B. // IEEE Transactions on Very Large Scale Integration (VLSI) Systems. - 2007. - Vol. 15, No. 4. - P. 465-470.

J468. Malik H.M.A. Robust Data Hiding in Audio Using Allpass Filters. / Malik H.M.A., Ansari R., Khokhar A.A. // IEEE Transactions on Audio, Speech, and Language Processing. - 2007. - Vol. 15, No. 4. - P. 1296-1304.

J469. Chun-Shien Lu. Near-Optimal Watermark Estimation and Its Countermeasure: Antidisclosure Watermark for Multiple Watermark Embedding. / Chun-Shien Lu, Chao-Yung Hsu. // IEEE Transactions on Circuits and Systems for Video Technology. - 2007. - Vol. 17, No. 4. - P. 454-467.

J470. Vazquez E. A New Approach Traveling-Wave Distance Protection—Part I: Algorithm. / Vazquez E., Castruita J., Chacon O.L., Conde A. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 2. - P. 795-800.

J471. Budgen D. A Data Integration Broker for Healthcare Systems. / Budgen D., Rigby M., Brereton P., Turner M. // Computer. - 2007. - Vol. 40, No. 4. - P. 34-41.

J472. Diaz C.S. The Technical Writer's Role in Preserving Intellectual Property Rights Outside the United States Tutorial. IEEE Transactions on Professional Communication. - 2007. - Vol. 50, No. 2. - P. 121-129.

J473. Changcheng Huang. A Scalable Path Protection Mechanism for Guaranteed Network Reliability Under Multiple Failures. / Changcheng Huang, Minzhe Li, Srinivasan A. // IEEE Transactions on Reliability. - 2007. - Vol. 56, No. 2. - P. 254-267.

J474. Hars L. Discryption: Internal Hard-Disk Encryption for Secure Storage. Computer. - 2007. - Vol. 40, No. 6. - P. 103-105.

J475. Swart R.S. Educating Students to Create Trustworthy Systems. / Swart R.S., Erbacher R.F. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 3. - P. 58-61.

J476. Knutson T.R. Building Privacy into Software Products and Services. IEEE Security & Privacy. - 2007. - Vol. 5, No. 3. - P. 72-74.

J477. Gagnon M.N. Software Protection through Anti-Debugging. / Gagnon M.N., Taylor S., Ghosh A.K. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 3. - P. 82-84.

J478. Price S.M. Supporting Resource-Constrained Collaboration Environments. Computer. - 2007. - Vol. 40, No. 6. - P. 108-107.

J479. Su Sheng. Context Information-Based Cyber Security Defense of Protection System. / Su Sheng, Chan W.L., Li K.K., Duan Xianzhong, Zeng Xiangjun. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 3. - P. 1477-1481.

J480. Telang Rahul. An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. / Telang Rahul, Wattal Sunil. // IEEE Transactions on Software Engineering. - 2007. - Vol. 33, No. 8. - P. 544-557.

J481. Boyce R.D. Modeling Drug Mechanism Knowledge Using Evidence and Truth Maintenance. / Boyce R.D., Collins C., Horn J., Kalet I. // IEEE Transactions on Information Technology in Biomedicine. - 2007. - Vol. 11, No. 4. - P. 386-397.

J482. Sundeep B. Self-Orthogonality of q -Ary Images of qm -Ary Codes and Quantum Code Construction. / Sundeep B, Thangaraj A. // IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 7. - P. 2480-2489.

J483. Ching-Lai Hor. Building Knowledge for Substation-Based Decision Support Using Rough Sets. / Ching-Lai Hor, Crossley P.A., Watson S.J. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 3. - P. 1372-1379.

J484. Chang-Hyun Park. Stochastic Estimation of Voltage Sags in a Large Meshed Network. / Chang-Hyun Park, Gilsoo Jang. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 3. - P. 1655-1664.

J485. Trope R.L. A Coherent Strategy for Data Security through Data Governance. / Trope R.L., Power E.M., Polley V.I., Morley B.C. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 3. - P. 32-39.

J486. Huang S. Optical Watermarking for Printed Document Authentication. / Huang S., Wu J.K. // IEEE

Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 2. - P. 164-173.

J487. Sun Y.L. Analysis and Protection of Dynamic Membership Information for Group Key Distribution Schemes. / Sun Y.L., Liu K.J.R. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 2. - P. 213-226.

J488. Yu W. Securing Cooperative Ad-Hoc Networks Under Noise and Imperfect Monitoring: Strategies and Game Theoretic Analysis. / Yu W., Ji Z., Liu K.J.R. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 2. - P. 240-253.

J489. Chen C.-L. Simulated annealing-based optimal wind-thermal coordination scheduling. IET Generation, Transmission & Distribution. - 2007. - Vol. 1, No. 3. - P. 447-455.

J490. Ik Rae Jeong. Strong Diffie-Hellman-DSA Key Exchange. / Ik Rae Jeong, Jeong Ok Kwon, Dong Hoon Lee. // IEEE Communications Letters. - 2007. - Vol. 11, No. 5. - P. 432-433.

J491. Furon T. A Constructive and Unifying Framework for Zero-Bit Watermarking. IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 2. - P. 149-163.

J492. Fu F. Noncollaborative Resource Management for Wireless Multimedia Applications Using Mechanism Design. / Fu F., van der Schaar M. // IEEE Transactions on Multimedia. - 2007. - Vol. 9, No. 4. - P. 851-868.

J493. Lawrence Pfleeger Shari. Guest Editors' Introduction: Managing Organizational Security. / Lawrence Pfleeger Shari, Trope Roland L., Palmer Charles C. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 3. - P. 13-15.

J494. Johnson M.E. Embedding Information Security into the Organization. / Johnson M.E., Goetz E. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 3. - P. 16-24.

J495. Pfleeger S.L. I'll Buy That! Cybersecurity in the Internet Marketplace. / Pfleeger S.L., Libicki M., Webber M. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 3. - P. 25-31.

J496. Qian Xu. Distributed Joint Source-Channel Coding of Video Using Raptor Codes. / Qian Xu, Stankovic V., Zixiang Xiong. // IEEE Journal on Selected Areas in Communications. - 2007. - Vol. 25, No. 4. - P. 851-861.

J497. Liu Y. Spare Capacity Allocation in Two-Layer Networks. / Liu Y., Tipper D., Vajanapoom K. // IEEE Journal on Selected Areas in Communications. - 2007. - Vol. 25, No. 5. - P. 974-986.

J498. Ingram M. Toward effective substation automation. / Ingram M., Ehlers R. // IEEE Power and Energy Magazine. - 2007. - Vol. 5, No. 3. - P. 67-73.

J499. Nan Zhang. Transmission Line Boundary Protection Using Wavelet Transform and Neural Network. / Nan Zhang, Kezunovic M. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 2. - P. 859-869.

J500. Landwehr C.E. New Challenges for the New Year. IEEE Security & Privacy. - 2007. - Vol. 5, No. 1. - P. 3-4.

J501. Wade H. Baker. Is Information Security Under Control?: Investigating Quality in Information Security Management. / Wade H. Baker, Linda Wallace. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 1. - P. 36-44.

J502. Reisman S. Slaying the Academia Beast [The Ivory Tower]. IT Professional. - 2007. - Vol. 9, No. 1. - P. 64.

J503. Vinton G. Cerf. An Information Avalanche. Computer. - 2007. - Vol. 40, No. 1. - P. 104-105.

J504. Rustam Stolkin. Using Environmental Models to Optimize Sensor Placement. / Rustam Stolkin, Lucas Vickers, Jeffrey V. Nickerson. // IEEE Sensors Journal. - 2007. - Vol. 7, No. 3. - P. 319-320.

J505. Ashwin Swaminathan. Nonintrusive Component Forensics of Visual Sensors Using Output Images. / Ashwin Swaminathan, Min Wu, K. J. Ray Liu. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 1. - P. 91-106.

J506. Jiantao Zhou. Security Analysis of Multimedia Encryption Schemes Based on Multiple Huffman Table. / Jiantao Zhou, Zhiqin Liang, Yan Chen, Oscar C. Au. // IEEE Signal Processing Letters. - 2007. - Vol. 14, No. 3. - P. 201-204.

J507. Maneli Noorkami. A Framework for Robust Watermarking of H.264-Encoded Video With Controllable Detection Performance. / Maneli Noorkami, Russell M. Mersereau. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 1. - P. 14-23.

J508. Annie I. Anton. HIPAA's Effect on Web Site Privacy Policies. / Annie I. Anton, Julia B. Eart, Matthew W. Vail, Neha Jain, Carrie M. Gheen, Jack M. Frink. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 1. - P. 45-52.

J509. Tsung-Yuan Liu. A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique. / Tsung-Yuan Liu, Wen-Hsiang Tsai. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 1. - P. 24-30.

J510. Qingfu Zhang. Evolutionary Algorithms Refining a Heuristic: A Hybrid Method for Shared-Path Protections in WDM Networks Under SRLG Constraints. / Qingfu Zhang, Jianyong Sun, Gaoxi Xiao, Tsang E. // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. - 2007. - Vol. 37, No. 1. - P. 51-61.

J511. van der Schaar M. Cross-Layer Packetization and Retransmission Strategies for Delay-Sensitive Wireless Multimedia Transmission. / van der Schaar M., Turaga D. S. // IEEE Transactions on Multimedia. - 2007. - Vol. 9, No. 1. - P. 185-197.

J512. Zhu B. Render Sequence Encoding for Document Protection. / Zhu B., Wu J., Kankanhalli M. S. // IEEE Transactions on Multimedia. - 2007. - Vol. 9, No. 1. - P. 16-24.

J513. Lickel Charles W. Introduction. IBM Systems Journal. - 2007. - Vol. 46, No. 2. - P. 1.

J514. Kudo M. Best practices and tools for personal information compliance management. / Kudo M., Araki Y., Nomiyama H., Saito S., Sohda Y. // IBM Systems Journal. - 2007. - Vol. 46, No. 2. - P. 235-253.

J515. Johnson C. M. Compliance with data protection laws using Hippocratic Database active enforcement and auditing. / Johnson C. M., Grandison T. W. A. // IBM Systems Journal. - 2007. - Vol. 46, No. 2. - P. 255-264.

J516. Nelson Theethayi. Experimental Investigation of Lightning Transients Entering a Swedish Railway Facility. / Nelson Theethayi, Rajeev Thottappillil, Tegegne Yirdaw, Yaqing Liu, Thomas Gotschl, Raul Montano. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 1. - P. 354-363.

J517. {no data available}. Bosch wireless IP solution provides crime protection [Briefing contracts]. Information Professional. - 2007. - Vol. 4, No. 3. - P. 12-13.

J518. Natthaphob Nimpitiwan. Fault Current Contribution From Synchronous Machine and Inverter Based Distributed Generators. / Natthaphob Nimpitiwan, Gerald Thomas Heydt, Raja Ayyanar, Siddharth Suryanarayanan. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 1. - P. 634-641.

J519. Habib M. K. Fiber-Grating-Based Vision System for Real-Time Tracking, Monitoring, and Obstacle Detection. IEEE Sensors Journal. - 2007. - Vol. 7, No. 1. - P. 105-121.

J520. Tai Nengling. Differential Protection Based on Zero-Sequence Voltages for Generator Stator Ground Fault. / Tai Nengling, Juergen Stenzel. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 1. - P. 116-121.

J521. Gangadharan P.K. Influence of current transformer saturation on line current differential protection algorithms. / Gangadharan P.K., Sidhu T.S., Klimek A. // IET Generation, Transmission & Distribution. - 2007. - Vol. 1, No. 2. - P. 270-277.

J522. Samantaray S.R. Power transformer protection using S-transform with complex window and pattern recognition approach. / Samantaray S.R., Panigrahi B.K., Dash P.K., Panda G. // IET Generation, Transmission & Distribution. - 2007. - Vol. 1, No. 2. - P. 278-286.

J523. Fung B.C.M. Anonymizing Classification Data for Privacy Preservation. / Fung B.C.M., Wang K., Yu P.S. // IEEE Transactions on Knowledge and Data Engineering. - 2007. - Vol. 19, No. 5. - P. 711-725.

J524. Krotov D.S. On Z2k -Dual Binary Codes. IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 4. - P. 1532-1537.

J525. Rahnavard N. Rateless Codes With Unequal Error Protection Property. / Rahnavard N., Vellambi B.N., Fekri F. // IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 4. - P. 1521-1532.

J526. Lesk M. South Korea's Way to the Future. IEEE Security & Privacy. - 2007. - Vol. 5, No. 2. - P. 85-87.

J527. El-Arroudi K. Intelligent-Based Approach to Islanding Detection in Distributed Generation. / El-Arroudi K., Joos G., Kamwa I., McGillis D.T. // IEEE Transactions on Power Delivery. - 2007. - Vol. 22, No. 2. - P. 828-835.

J528. Power E.M. Setting Boundaries at Borders: Reconciling Laptop Searches and Privacy. / Power E.M., Gilhen J., Trope R.L. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 2. - P. 72-75.

J529. Jung-Tae Kim. Implementation of the DLNA Proxy System for Sharing Home Media Contents. / Jung-Tae Kim, Yeon-Joo Oh, Hoon-Ki Lee, Eui-Hyun Paik, Kwang-Roh Park. // IEEE Transactions on Consumer Electronics. - 2007. - Vol. 53, No. 1. - P. 139-144.

J530. Bhargav-Spantzel A. Trust Negotiation in Identity Management. / Bhargav-Spantzel A., Squicciarini A.C., Bertino E. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 2. - P. 55-63.

J531. Lei Guo. On Finding Feasible Solutions With Shared Backup Resources for Surviving Double-Link Failures in Path-Protected WDM Mesh Networks. / Lei Guo, Li L., Jin Cao, Hongfang Yu, Xuetao Wei. // Journal of Lightwave Technology. - 2007. - Vol. 25, No. 1. - P. 287-296.

J532. Pooya Forghani-zadeh H. An Accurate, Continuous, and Lossless Self-Learning CMOS Current-Sensing Scheme for Inductor-Based DC-DC Converters. / Pooya Forghani-zadeh H., Rincon-Mora G.A. // IEEE Journal of Solid-State Circuits. - 2007. - Vol. 42, No. 3. - P. 665-679.

J533. Cholda P. Comments on "On Hamiltonian Cycles as Optimal p-Cycles". IEEE Communications Letters. - 2007. - Vol. 11, No. 2. - P. 200.

J534. G. David Forney. Convolutional and Tail-Biting Quantum Error-Correcting Codes. / G. David Forney, Markus Grassl, Saikat Guha. // IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 3. - P. 865-880.

J535. Haining Wang. Defense Against Spoofed IP Traffic Using Hop-Count Filtering. / Haining Wang, Cheng Jin, Kang G. Shin. // IEEE/ACM Transactions on Networking. - 2007. - Vol. 15, No. 1. - P. 40-53.

J536. Pradhan A.K. Adaptive Distance Relay Setting for Lines Connecting Wind Farms. / Pradhan A.K., Joos G. // IEEE Transactions on Energy Conversion. - 2007. - Vol. 22, No. 1. - P. 206-213.

J537. Laird C. Taking a Hard-Line Approach to Encryption. Computer. - 2007. - Vol. 40, No. 3. - P. 13-15.

J538. Stahl B.C. Privacy and security as ideology. IEEE Technology and Society Magazine. - 2007. - Vol. 26, No. 1. - P. 35-45.

J539. Zhenwei Yu. An Automatically Tuning Intrusion Detection System. / Zhenwei Yu, Tsai J.J.P., Weigert T. // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. - 2007. - Vol. 37, No. 2. - P. 373-384.

J540. van der Merwe J. A Fully Distributed Proactively Secure Threshold-Multisignature Scheme. / van der Merwe J., Dawoud D.S., McDonald S. // IEEE Transactions on Parallel and Distributed Systems. - 2007. - Vol. 18, No. 4. - P. 562-575.

J541. Beatty P. P3P Adoption on E-Commerce Web sites: A Survey and Analysis. / Beatty P., Reay I., Dick S., Miller J. // IEEE Internet Computing. - 2007. - Vol. 11, No. 2. - P. 65-71.

J542. Lingling Pu. Joint Source-Channel Rate Allocation in Parallel Channels. / Lingling Pu, Marcellin M.W., Djordjevic I., Vasic B., Bilgin A. // IEEE Transactions on Image Processing. - 2007. - Vol. 16, No. 8. - P. 2016-2022.

J543. Shan He. Collusion-Resistant Video Fingerprinting for Large User Group. / Shan He, Min Wu. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 4. - P. 697-709.

J544. Nandakumar K. Fingerprint-Based Fuzzy Vault: Implementation and Performance. / Nandakumar K., Jain A.K., Pankanti S. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 4. - P. 744-757.

J545. Weitzner D.J. Google, Profiling, and Privacy. IEEE Internet Computing. - 2007. - Vol. 11, No. 6. - P. 95-96, c3.

J546. Karam L.J. Selective Error Detection for Error-Resilient Wavelet-Based Image Coding. / Karam L.J., Tuyet-Trang Lam. // IEEE Transactions on Image Processing. - 2007. - Vol. 16, No. 12. - P. 2936-2942.

J547. Mansmann F. Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats. / Mansmann F., Keim D.A., North S.C., Rexroad B., Sheleheda D. // IEEE Transactions on Visualization and Computer Graphics. - 2007. - Vol. 13, No. 6. - P. 1105-1112.

J548. Mekic F. Protecting a High Horsepower Motor. / Mekic F., Gaynor P.A., Wilson R.A. // IEEE Industry Applications Magazine. - 2007. - Vol. 13, No. 6. - P. 50-57.

J549. Davidson M.A. Enterprise Security for Web 2.0. / Davidson M.A., Yoran E. // Computer. - 2007. - Vol. 40, No. 11. - P. 117-119.

J550. Stamatiou K. Performance Analysis of a Coherent FH-MA System Based on Latin Squares. / Stamatiou K., Proakis J.G. // IEEE Transactions on Wireless Communications. - 2007. - Vol. 6, No. 11. - P. 4183-4192.

J551. Langheinrich M. Practical Minimalist Cryptography for RFID Privacy. / Langheinrich M., Marti R. // IEEE Systems Journal. - 2007. - Vol. 1, No. 2. - P. 115-128.

J552. Wei Liu. Optimum Detection for Spread-Spectrum Watermarking That Employs Self-Masking. / Wei Liu, Lina Dong, Wenjun Zeng. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 4. - P. 645-654.

J553. Otomega B. Undervoltage Load Shedding Using Distributed Controllers. / Otomega B., Van Cutsem T. // IEEE Transactions on Power Systems. - 2007. - Vol. 22, No. 4. - P. 1898-1907.

J554. Otomega B. Distributed Undervoltage Load Shedding. / Otomega B., Glavic M., Van Cutsem T. // IEEE Transactions on Power Systems. - 2007. - Vol. 22, No. 4. - P. 2283-2284.

J555. Patrikakis C. Security and Privacy in Pervasive Computing. / Patrikakis C., Karamolegkos P., Voulodimos A. // IEEE Pervasive Computing. - 2007. - Vol. 6, No. 4. - P. 73-75.

J556. Zan Huang. A Comparison of Collaborative-Filtering Recommendation Algorithms for E-commerce. / Zan Huang, Zeng D., Hsinchun Chen. // IEEE Intelligent Systems. - 2007. - Vol. 22, No. 5. - P. 68-78.

J557. Kriplean T. Physical Access Control for Captured RFID Data. / Kriplean T., Welbourne E., Khoussainova N., Rastogi V., Balazinska M., Borriello C., Kohno T., Suciu D. // IEEE Pervasive Computing. - 2007. - Vol. 6, No. 4. - P. 48-55.

J558. Kirbiz S. Decode-Time Forensic Watermarking of AAC Bitstreams. / Kirbiz S., Lemma A.N., Celik M.U., Katzenbeisser S. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 4. - P. 683-696.

J559. Mulan Liu. Multiplicative Linear Secret Sharing Schemes Based on Connectivity of Graphs. / Mulan Liu, Liangliang Xiao, Zhifang Zhang. // IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 11. - P. 3973-3978.

J560. Xiaolin Tong. Distortion-Driven Video Streaming over Multihop Wireless Networks with Path Diversity. / Xiaolin Tong, Andreopoulos Y., van der Schaar M. // IEEE Transactions on Mobile Computing. - 2007. - Vol. 6,

No. 12. - P. 1343-1356.

J561. Cheema U. Expert Systems for Earthquake Damage Assessment. IEEE Aerospace and Electronic Systems Magazine. - 2007. - Vol. 22, No. 9. - P. 6-10.

J562. Cardarilli G.C. Analysis of Errors and Erasures in Parity Sharing RS Codecs. / Cardarilli G.C., Pontarelli S., Re M., Salsano A. // IEEE Transactions on Computers. - 2007. - Vol. 56, No. 12. - P. 1721-1726.

J563. Faldum A. On the Trustworthiness of Error-Correcting Codes. IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 12. - P. 4777-4784.

J564. Vaudenay S. E-Passport Threats. IEEE Security & Privacy. - 2007. - Vol. 5, No. 6. - P. 61-64.

J565. Stytz M.R. Who Are the Experts, and What Have They Done for Us Lately?. IEEE Security & Privacy. - 2007. - Vol. 5, No. 6. - P. 78-80.

J566. Power E.M. Developing a Culture of Privacy: A Case Study. IEEE Security & Privacy. - 2007. - Vol. 5, No. 6. - P. 58-60.

J567. Jakobsson M. Web Camouflage: Protecting Your Clients from Browser-Sniffing Attacks. / Jakobsson M., Stamm S. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 6. - P. 16-24.

J568. Hole K.J. Lessons from the Norwegian ATM System. / Hole K.J., Moen V., Klingsheim A.N., Tande K.M. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 6. - P. 25-31.

J569. Paradelo Junior Romildo de Campos. Overcurrent Protection in Electrical Distribution Systems Through Probabilistic Approach. / Paradelo Junior Romildo de Campos, Schmidt Hernan Prieto. // IEEE (Revista IEEE America Latina) Latin America Transactions. - 2007. - Vol. 5, No. 8. - P. 599-604.

J570. Hartong M. Key management requirements for PTC operations. / Hartong M., Goel R., Wijesekera D. // IEEE Vehicular Technology Magazine. - 2007. - Vol. 2, No. 2. - P. 4-11.

J571. Gueron S. Where Does Security Stand? New Vulnerabilities vs. Trusted Computing. / Gueron S., Stronqin G., Seifert J.-P., Chiou D., Sendag R., Yi J.J. // IEEE Micro. - 2007. - Vol. 27, No. 6. - P. 25-35.

J572. Bishop M. About Penetration Testing. IEEE Security & Privacy. - 2007. - Vol. 5, No. 6. - P. 84-87.

J573. Lee P.P.C. Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks. / Lee P.P.C., Misra V., Rubenstein D. // IEEE/ACM Transactions on Networking. - 2007. - Vol. 15, No. 6. - P. 1490-1501.

J574. Bo Sun. Intrusion detection techniques in mobile ad hoc and wireless sensor networks. / Bo Sun, Osborne L., Yang Xiao, Guizani S. // IEEE Wireless Communications. - 2007. - Vol. 14, No. 5. - P. 56-63.

J575. Schaumont Patrick. Guest Editors' Introduction: Security and Trust in Embedded-Systems Design. / Schaumont Patrick, Raghunathan Anand. // IEEE Design & Test of Computers. - 2007. - Vol. 24, No. 6. - P. 518-520.

J576. Yi Qian. A design for secure and survivable wireless sensor networks. / Yi Qian, Kejie Lu, Tipper D. // IEEE Wireless Communications. - 2007. - Vol. 14, No. 5. - P. 30-37.

J577. Hongbin Luo. Achieving Shared Protection for Dynamic Multicast Sessions in Survivable Mesh WDM Networks. / Hongbin Luo, Lemin Li, Hongfang Yu, Sheng Wang. // IEEE Journal on Selected Areas in Communications. - 2007. - Vol. 25, No. 9. - P. 83-95.

J578. Dieu-Linh Truong. Using Topology Aggregation for Efficient Shared Segment Protection Solutions in Multi-Domain Networks. / Dieu-Linh Truong, Jaumard B. // IEEE Journal on Selected Areas in Communications. - 2007. - Vol. 25, No. 9. - P. 96-107.

J579. Mihm Tom. Protecting Critical Data. IEEE Design & Test of Computers. - 2007. - Vol. 24, No. 6. - P. 592.

J580. Mihaljevic M.J. Security evaluation of certain broadcast encryption schemes employing a generalized

time-memory-data trade-off. / Mihaljevic M.J., Fossorier M.P.C., Imai H. // IEEE Communications Letters. - 2007. - Vol. 11, No. 12. - P. 988-990.

J581. Trimberger S. Security in SRAM FPGAs. IEEE Design & Test of Computers. - 2007. - Vol. 24, No. 6. - P. 581.

J582. Popp T. Power Analysis Attacks and Countermeasures. / Popp T., Oswald E., Mangard S. // IEEE Design & Test of Computers. - 2007. - Vol. 24, No. 6. - P. 535-543.

J583. Chong Hee Kim. Faults, Injection Methods, and Fault Attacks. / Chong Hee Kim, Quisquater J.-J. // IEEE Design & Test of Computers. - 2007. - Vol. 24, No. 6. - P. 544-545.

J584. Zeng D. Protecting Transportation Infrastructure. / Zeng D., Chawathe S.S., Hua Huang, Fei-Yue Wang. // IEEE Intelligent Systems. - 2007. - Vol. 22, No. 5. - P. 8-11.

J585. Badishi G. Keeping Denial-of-Service Attackers in the Dark. / Badishi G., Herzberg A., Idit K. // IEEE Transactions on Dependable and Secure Computing. - 2007. - Vol. 4, No. 3. - P. 191-204.

J586. Tairan Wang. Multi-Tier Cooperative Broadcasting with Hierarchical Modulations. / Tairan Wang, Cano A., Giannakis G.B., Ramos J. // IEEE Transactions on Wireless Communications. - 2007. - Vol. 6, No. 8. - P. 3047-3057.

J587. Yanchao Zhang Y. A Fine-Grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks. / Yanchao Zhang Y., Yuguang Fang Y. // IEEE Transactions on Parallel and Distributed Systems. - 2007. - Vol. 18, No. 8. - P. 1134-1145.

J588. Heikkila Faith M. Encryption: Security Considerations for Portable Media Devices. IEEE Security & Privacy. - 2007. - Vol. 5, No. 4. - P. 22-27.

J589. Veld S.I. Data Sharing across the Atlantic. IEEE Security & Privacy. - 2007. - Vol. 5, No. 4. - P. 58-61.

J590. XiaoTong Wang. Reversible Data-Hiding Scheme for 2-D Vector Maps Based on Difference Expansion. / XiaoTong Wang, ChengYong Shao, XiaoGang Xu, XiaMu Niu. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 3. - P. 311-320.

J591. Jidong Zhong. Double-Sided Watermark Embedding and Detection. / Jidong Zhong, Shangteng Huang. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 3. - P. 297-310.

J592. Yagiz Sutcu. Protecting Biometric Templates With Sketch: Theory and Practice. / Yagiz Sutcu, Qiming Li, Memon N. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 3. - P. 503-512.

J593. Bhanu B. Guest Editorial: Special Issue on Human Detection and Recognition. / Bhanu B, Ratha N. K., Kumar V, Chellappa R, Bigun J. // IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 3. - P. 489-490.

J594. Frattolillo F. Watermarking Protocol for Web Context. IEEE Transactions on Information Forensics and Security. - 2007. - Vol. 2, No. 3. - P. 350-363.

J595. Stankovic V. Distributed Source Coding for Multimedia Multicast Over Heterogeneous Networks. / Stankovic V., Yang Yang, Zixiang Xiong. // IEEE Journal of Selected Topics in Signal Processing. - 2007. - Vol. 1, No. 2. - P. 220-230.

J596. El-Arroudi K. Data Mining Approach to Threshold Settings of Islanding Relays in Distributed Generation. / El-Arroudi K., Joos G. // IEEE Transactions on Power Systems. - 2007. - Vol. 22, No. 3. - P. 1112-1119.

J597. Hoi Yin Shutoy. Cooperative Source and Channel Coding for Wireless Multimedia Communications. / Hoi Yin Shutoy, Gunduz D., Erkip E., Yao Wang. // IEEE Journal of Selected Topics in Signal Processing. - 2007. - Vol. 1, No. 2. - P. 295-307.

J598. Doncel V.R. An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics. / Doncel V.R., Nikolaidis N., Pitas I. // IEEE Transactions on Visualization and Computer Graphics. - 2007. - Vol. 13, No. 5. - P. 851-863.

J599. Ould-Cheikh-Mouhamedou Y. Improving the Error Rate Performance of Turbo Codes using the Forced Symbol Method. / Ould-Cheikh-Mouhamedou Y., Crozier S. // IEEE Communications Letters. - 2007. - Vol. 11, No. 7. - P. 616-618.

J600. Ortega Brandi. News Briefs. IEEE Security & Privacy. - 2007. - Vol. 5, No. 4. - P. 6-9.

J601. English J. MEMS-Assisted Cryptography for CPI Protection. / English J., Coe D., Gaede R., Hyde D., Kulick J. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 4. - P. 14-21.

J602. Trevor J. AnySpot: Pervasive Document Access and Sharing. / Trevor J., Hilbert D.M. // IEEE Pervasive Computing. - 2007. - Vol. 6, No. 3. - P. 76-84.

J603. Dahai Xu. Ultrafast Potential-Backup-Cost (PBC)-Based Shared Path Protection Schemes. / Dahai Xu, Chunming Qiao, Yizhi Xiong. // Journal of Lightwave Technology. - 2007. - Vol. 25, No. 8. - P. 2251-2259.

J604. Pereira Z.C. Unequal error protection for LZSS compressed data using Reed-Solomon codes. / Pereira Z.C., Pellenz M.E., Souza R.D., Siqueira M.A.A. // IET Communications. - 2007. - Vol. 1, No. 4. - P. 612-617.

J605. Aguirre M.A. Selective Protection Analysis Using a SEU Emulator: Testing Protocol and Case Study Over the Leon2 Processor. / Aguirre M.A., Tombs J.N., Muoz F., Baena V., Guzman H., Napoles J., Torralba A., Fernandez-Leon A., Tortosa-Lopez F., Merodio D. // IEEE Transactions on Nuclear Science. - 2007. - Vol. 54, No. 4. - P. 951-956.

J606. Weitzner D.J. Beyond Secrecy: New Privacy Protection Strategies for Open Information Spaces. IEEE Internet Computing. - 2007. - Vol. 11, No. 5. - P. 96-95.

J607. Xinpeng Zhang. Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels. / Xinpeng Zhang, Shuozhong Wang. // IEEE Signal Processing Letters. - 2007. - Vol. 14, No. 10. - P. 727-730.

J608. Hsien-Po Shiang. Informationally Decentralized Video Streaming Over Multihop Wireless Networks. / Hsien-Po Shiang, van der Schaar M. // IEEE Transactions on Multimedia. - 2007. - Vol. 9, No. 6. - P. 1299-1313.

J609. Daewon Song. Scalable H.264/AVC Video Transmission Over MIMO Wireless Systems With Adaptive Channel Selection Based on Partial Channel Information. / Daewon Song, Chang Wen Chen. // IEEE Transactions on Circuits and Systems for Video Technology. - 2007. - Vol. 17, No. 9. - P. 1218-1226.

J610. Dushin F. Handling Multiple Credentials in a Heterogeneous SOA Environment. / Dushin F., Newcomer E. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 5. - P. 80-82.

J611. Solomon D. Balancing Privacy and Risk in the E-Messaging World. IEEE Security & Privacy. - 2007. - Vol. 5, No. 5. - P. 72-75.

J612. Gratzer V. Trust on a Nationwide Scale. / Gratzer V., Naccache D. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 5. - P. 69-71.

J613. Puducheri S. The Design and Performance of Distributed LT Codes. / Puducheri S., Kliewer J., Fuja T.E. // IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 10. - P. 3740-3754.

J614. Fraser D. The Canadian Response to the USA Patriot Act. IEEE Security & Privacy. - 2007. - Vol. 5, No. 5. - P. 66-68.

J615. D'Amico A.D. Visual Discovery in Computer Network Defense. / D'Amico A.D., Goodall J.R., Tesone D.R., Kopylec J.K. // IEEE Computer Graphics and Applications. - 2007. - Vol. 27, No. 5. - P. 20-27.

J616. Nishimoto Y. Advanced Conditional Access System for Digital Broadcasting Receivers Using Metadata. / Nishimoto Y., Baba A., Kimura T., Imaizumi H., Fujita Y. // IEEE Transactions on Broadcasting. - 2007. - Vol. 53, No. 3. - P. 697-702.

J617. Flanagin M. Hydraulic Splines: A Hybrid Approach to Modeling River Channel Geometries. / Flanagin M., Grenotton A., Ratcliff J., Shaw K.B., Sample J., Abdelguerfi M. // Computing in Science & Engineering. - 2007. - Vol. 9, No. 5. - P. 4-15.

J618. Ross R. Managing Enterprise Security Risk with NIST Standards. Computer. - 2007. - Vol. 40, No. 8. - P. 88-91.

J619. El-Alfy El-Sayed M. A Review of Network Security. IEEE Distributed Systems Online. - 2007. - Vol. 8, No. 7. - P. 6.

J620. Oggier F. Cyclic Algebras for Noncoherent Differential Space-Time Coding. IEEE Transactions on Information Theory. - 2007. - Vol. 53, No. 9. - P. 3053-3065.

J621. Cousins T.J. Devising Post-Disaster Continuity Plans that Meet Actual Recovery Needs. IEEE Technology and Society Magazine. - 2007. - Vol. 26, No. 3. - P. 13-23.

J622. Ferraro P.B. A System for the Measurement of the Amazon. / Ferraro P.B., Bauersachs M., Burns J., Bataller G. // IEEE Aerospace and Electronic Systems Magazine. - 2007. - Vol. 22, No. 8. - P. 9-19.

J623. Mullins B.E. How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum. / Mullins B.E., Lacey T.H., Mills R.F., Trechter J.M., Bass S.D. // IEEE Security & Privacy. - 2007. - Vol. 5, No. 5. - P. 40-49.

J624. Metwally I.A. Computation of Transient Overvoltages in Low-Voltage Installations During Direct Strikes to Different Lightning Protection Systems. / Metwally I.A., Heidler F.H. // IEEE Transactions on Electromagnetic Compatibility. - 2007. - Vol. 49, No. 3. - P. 602-613.

J625. Yi Lu. Trust-based privacy preservation for peer-to-peer data sharing. / Yi Lu, Weichao Wang, Bhargava B., Dongyan Xu. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2006. - Vol. 36, No. 3. - P. 498-502.

J626. Schaathun H.G. The Boneh-Shaw fingerprinting scheme is better than we thought. IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 2. - P. 248-255.

J627. Karybali I.G. Efficient spatial image watermarking via new perceptual masking and blind detection schemes. / Karybali I.G., Berberidis K. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 2. - P. 256-274.

J628. Sullivan K. Steganalysis for Markov cover data with applications to images. / Sullivan K., Madhow U., Chandrasekaran S., Manjunath B.S. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 2. - P. 275-287.

J629. Lilien L. A scheme for privacy-preserving data dissemination. / Lilien L., Bhargava B. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2006. - Vol. 36, No. 3. - P. 503-506.

J630. Shan He. Joint coding and embedding techniques for MultimediaFingerprinting. / Shan He, Min Wu. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 2. - P. 231-247.

J631. Kuper P. A warning to industry-fix it or lose it. IEEE Security & Privacy. - 2006. - Vol. 4, No. 2. - P. 56-60.

J632. Rae A. Fault evaluation for security-critical communication devices. / Rae A., Fidge C., Wildman L. // Computer. - 2006. - Vol. 39, No. 5. - P. 61-68.

J633. Yoohwan Kim. PacketScore: a statistics-based packet filtering scheme against distributed denial-of-service attacks. / Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah, Chao H.J. // IEEE Transactions on Dependable and Secure Computing. - 2006. - Vol. 3, No. 2. - P. 141-155.

J634. Tarn J.M. Mobile technology as a learning object and an exploration tool in an IS curriculum: an innovative instruction of wireless network security. / Tarn J.M., Kuanchin Chen. // IEEE Transactions on Education. - 2006. - Vol. 49, No. 2. - P. 193-198.

J635. Gennaro R. Randomness in cryptography. IEEE Security & Privacy. - 2006. - Vol. 4, No. 2. - P. 64-67.

J636. Davidson E.M. Applying multi-agent system technology in practice: automated management and analysis of SCADA and digital fault recorder data. / Davidson E.M., McArthur S.D.J., McDonald J.R., Cumming T., Watt I. // IEEE Transactions on Power Systems. - 2006. - Vol. 21, No. 2. - P. 559-567.

J637. Yongdong Wu. Nonlinear collusion attack on a watermarking scheme for buyer authentication. IEEE Transactions on Multimedia. - 2006. - Vol. 8, No. 3. - P. 626-629.

J638. Garfinkel R. Secure electronic markets for private information. / Garfinkel R., Gopal R.D., Nunez M., Rice D.O. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2006. - Vol. 36, No. 3. - P. 461-471.

J639. Arora H. Autonomic-computing approach to secure knowledge management: a game-theoretic analysis. / Arora H., Mishra B.K., Raghu T.S. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2006. - Vol. 36, No. 3. - P. 487-497.

J640. Bertino E. Secure knowledge management: confidentiality, trust, and privacy. / Bertino E., Khan L.R., Sandhu R., Thuraisingham B. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2006. - Vol. 36, No. 3. - P. 429-438.

J641. RaghavRao H. Part 1: Special Issue on Secure Knowledge Management. / RaghavRao H., Upadhyaya S.J. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2006. - Vol. 36, No. 3. - P. 418-420.

J642. Insu Park. Part 2: emerging issues for secure knowledge management-results of a Delphi study. / Insu Park, Jinkyu Lee, Upadhyaya S.J., Rao H.R. // IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. - 2006. - Vol. 36, No. 3. - P. 421-428.

J643. Houser D.S. A method for modeling marine mammal movement and behavior for environmental impact assessment. IEEE Journal of Oceanic Engineering. - 2006. - Vol. 31, No. 1. - P. 76-81.

J644. Subramanya S.R. Digital signatures. / Subramanya S.R., Yi B.K. // IEEE Potentials. - 2006. - Vol. 25, No. 2. - P. 5-8.

J645. M.H. Shwehdi. Reliable maps of lightning thunderstorms for Saudi Arabia. IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 3. - P. 1571-1577.

J646. Sidhu T.S. Series compensated line protection enhancement by modified pilot relaying schemes. / Sidhu T.S., Khederzadeh M. // IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 3. - P. 1191-1198.

J647. R. Giovanini. A primary and backup cooperative protection system based on wide area agents. / R. Giovanini, K. Hopkinson, D.V. Coury, J.S. Thorp. // IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 3. - P. 1222-1230.

J648. Schmidt K.-U. On cosets of the generalized first-order reed-muller code with low PMEPR. IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 7. - P. 3220-3232.

J649. Bross S.I. Improved upper bounds for codes with unequal error protection. / Bross S.I., Litsyn S. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 7. - P. 3329-3333.

J650. Sang-ho Park. Contents distribution system based on MPEG-4 ISMACryp in IP set-top box environments. / Sang-ho Park, Jaewoon Jeong, Taekyoung Kwon. // IEEE Transactions on Consumer Electronics. - 2006. - Vol. 52, No. 2. - P. 660-668.

J651. Subramanya S.R. Digital rights management. / Subramanya S.R., Yi B.K. // IEEE Potentials. - 2006. - Vol. 25, No. 2. - P. 31-34.

J652. {no data available}. Passwords and Passion. IEEE Software. - 2006. - Vol. 23, No. 4. - P. 5-7.

J653. Xie T. Scheduling security-critical real-time applications on clusters. / Xie T., Qin X. // IEEE Transactions on Computers. - 2006. - Vol. 55, No. 7. - P. 864-879.

J654. Garg N. Information Ethics: Privacy and Intellectual Property. IEEE Transactions on Professional

Communication. - 2006. - Vol. 49, No. 2. - P. 202-203.

J655. Stytz M.R. Dynamic software security testing. / Stytz M.R., Banks S.B. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 3. - P. 77-79.

J656. Bellia P.L. The fourth amendment and emerging communications technologies. IEEE Security & Privacy. - 2006. - Vol. 4, No. 3. - P. 20-28.

J657. Paterson K.G. Lost in translation: theory and practice in cryptography. / Paterson K.G., Yau A.K.L. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 3. - P. 69-72.

J658. Yong Sun. Progressive image transmission over space-time coded OFDM-based MIMO systems with adaptive modulation. / Yong Sun, Zixiang Xiong. // IEEE Transactions on Mobile Computing. - 2006. - Vol. 5, No. 8. - P. 1016-1028.

J659. West G.M. Data mining reactor fuel grab load trace data to support nuclear core condition monitoring. / West G.M., Jahn G.J., McArthur S.D.J., McDonald J.R., Reed J. // IEEE Transactions on Nuclear Science. - 2006. - Vol. 53, No. 3. - P. 1494-1503.

J660. Yinian Mao. A joint signal processing and cryptographic approach to multimedia encryption. / Yinian Mao, Min Wu. // IEEE Transactions on Image Processing. - 2006. - Vol. 15, No. 7. - P. 2061-2075.

J661. Freytes M. Resilient multicast conversational video. / Freytes M., Marques C.A. // IEEE Communications Letters. - 2006. - Vol. 10, No. 6. - P. 417-419.

J662. Hai Jiang. Resource allocation with service differentiation for wireless video transmission. / Hai Jiang, Weihua Zhuang. // IEEE Transactions on Wireless Communications. - 2006. - Vol. 5, No. 6. - P. 1456-1468.

J663. Pavlushkov V. Unequal error protection for convolutional codes. / Pavlushkov V., Johannesson R., Zyablov V.V. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 2. - P. 700-708.

J664. Perkins S. On an upper bound for mixed error-correcting codes. / Perkins S., Sakhnovich A.L., Smith D.H. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 2. - P. 708-712.

J665. Huntley C.L. A developmental view of system security. Computer. - 2006. - Vol. 39, No. 1. - P. 113-114.

J666. Yongdong Wu. Scalable authentication of MPEG-4 streams. / Yongdong Wu, Deng R.H. // IEEE Transactions on Multimedia. - 2006. - Vol. 8, No. 1. - P. 152-161.

J667. Ambainis A. The minimum distance problem for two-way entanglement purification. / Ambainis A., Gottesman D. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 2. - P. 748-753.

J668. Quan Zhou. Joint antenna selection and link adaptation for MIMO systems. / Quan Zhou, Huaiyu Dai. // IEEE Transactions on Vehicular Technology. - 2006. - Vol. 55, No. 1. - P. 243-255.

J669. Felten E.W. Digital rights management, spyware, and security. / Felten E.W., Halderman J.A. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 1. - P. 18-23.

J670. Davison R.M. Ethical values of IT professionals: evidence from Hong Kong. / Davison R.M., Martinsons M.G., Lo H.W.H., Kam C.S.P. // IEEE Transactions on Engineering Management. - 2006. - Vol. 53, No. 1. - P. 48-58.

J671. Jajszczyk A. Recovery of the control plane after failures in ASON/GMPLS networks. / Jajszczyk A., Rozycki P. // IEEE Network. - 2006. - Vol. 20, No. 1. - P. 4-10.

J672. Rosen G. Examining coding structure and redundancy in DNA. IEEE Engineering in Medicine and Biology Magazine. - 2006. - Vol. 25, No. 1. - P. 62-68.

J673. Fan Zhai. Rate-distortion optimized hybrid error control for real-time packetized video transmission. / Fan Zhai, Eisenberg Y., Pappas T.N., Berry R., Katsaggelos A.K. // IEEE Transactions on Image Processing. - 2006. - Vol. 15, No. 1. - P. 40-53.

J674. Thomos N. Optimized transmission of JPEG2000 streams over wireless channels. / Thomos N., Boulgouris N.V., Strintzis M.G. // IEEE Transactions on Image Processing. - 2006. - Vol. 15, No. 1. - P. 54-67.

J675. Capkun S. Mobility helps peer-to-peer security. / Capkun S., Hubaux J.P., Buttyan L. // IEEE Transactions on Mobile Computing. - 2006. - Vol. 5, No. 1. - P. 43-51.

J676. Zhao H.V. Fingerprint multicast in secure video streaming. / Zhao H.V., Liu K.J.R. // IEEE Transactions on Image Processing. - 2006. - Vol. 15, No. 1. - P. 12-29.

J677. Matsumoto T. Experience of numerical protective relays operating in an environment with high-frequency switching surge in Japan. / Matsumoto T., Kurosawa Y., Usui M., Yamashita K., Tanaka T. // IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 1. - P. 88-93.

J678. Park S.-J. Modelling and control of agent-based power protection systems using supervisors. / Park S.-J., Lim J.-T. // IEE Proceedings - Control Theory and Applications. - 2006. - Vol. 153, No. 1. - P. 92-98.

J679. Alghoniemy M. Progressive quantized projection approach to data hiding. / Alghoniemy M., Tewfik A.H. // IEEE Transactions on Image Processing. - 2006. - Vol. 15, No. 2. - P. 459-472.

J680. Hribernik W. Inherent transient recovery voltage of power transformers-a model-based determination procedure. / Hribernik W., Graber L., Brunke J.H. // IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 1. - P. 129-134.

J681. Merhav N. On joint coding for watermarking and encryption. IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 1. - P. 190-205.

J682. Sweeney L. Protecting job seekers from identity theft. IEEE Internet Computing. - 2006. - Vol. 10, No. 2. - P. 74-78.

J683. Liang Guishu. Calculation of transient radiation field from metallic enclosure of GIS based on surface-patch model. / Liang Guishu, Ran Huijuan, Dong Huaying, Cui Xiang. // IEEE Transactions on Magnetics. - 2006. - Vol. 42, No. 4. - P. 855-858.

J684. Harada M. Some restrictions on weight enumerators of singly even self-dual codes. / Harada M., Munemasa A. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 3. - P. 1266-1269.

J685. Kushner D. Uncommon law [copyright laws]. IEEE Spectrum. - 2006. - Vol. 43, No. 3. - P. 57-58.

J686. Sion R. Rights protection for discrete numeric streams. / Sion R., Atallah M., Prabhaka S. // IEEE Transactions on Knowledge and Data Engineering. - 2006. - Vol. 18, No. 5. - P. 699-714.

J687. Wenjun Zeng. Security for multimedia adaptation: architectures and solutions. / Wenjun Zeng, Junqiang Lan, Xinhua Zhuang. // IEEE Multimedia. - 2006. - Vol. 13, No. 2. - P. 68-76.

J688. Hwang D.D. Securing embedded systems. / Hwang D.D., Schaumont P., Tiri K., Verbauwhede I. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 2. - P. 40-49.

J689. Li M. Disenrollment with perfect forward secrecy in threshold schemes. / Li M., Poovendran R. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 4. - P. 1676-1682.

J690. Goth G. News: data-driven enterprise-slouching toward the semantic Web. IEEE Distributed Systems Online. - 2006. - Vol. 7, No. 3. - {no data available}.

J691. Tan L. Architectures for Bit-Split String Scanning in Intrusion Detection. / Tan L., Sherwood T. // IEEE Micro. - 2006. - Vol. 26, No. 1. - P. 110-117.

J692. Hao Yang. SCAN: self-organized network-layer security in mobile ad hoc networks. / Hao Yang, Shu J., Xiaoqiao Meng, Songwu Lu. // IEEE Journal on Selected Areas in Communications. - 2006. - Vol. 24, No. 2. - P. 261-273.

J693. Squicciarini A.C. Achieving privacy in trust negotiations with an ontology-based approach. / Squicciarini A.C., Bertino E., Ferrari E., Ray I. // IEEE Transactions on Dependable and Secure Computing. - 2006. - Vol. 3,

No. 1. - P. 13-30.

J694. Black J. A security analysis of the Internet Chess Club. / Black J., Cochran M., Gardner R. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 1. - P. 46-52.

J695. Chandramouli R. Challenges in securing the domain name system. / Chandramouli R., Rose S. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 1. - P. 84-87.

J696. Ran-Zan Wang. High-payload image steganography using two-way block matching. / Ran-Zan Wang, Yeh-Shun Chen. // IEEE Signal Processing Letters. - 2006. - Vol. 13, No. 3. - P. 161-164.

J697. Markel M. Safe harbor and privacy protection: a looming issue for IT professionals. IEEE Transactions on Professional Communication. - 2006. - Vol. 49, No. 1. - P. 1-11.

J698. Taney F.X. Securing the whole enterprise: business and legal issues. / Taney F.X., Costello T. // IT Professional. - 2006. - Vol. 8, No. 1. - P. 37-42.

J699. Boncelet C.G. Jr. The NTMAC for authentication of noisy messages. IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 1. - P. 35-42.

J700. Schainker R. Electric utility responses to grid security issues. / Schainker R., Douglas J., Kropp T. // IEEE Power and Energy Magazine. - 2006. - Vol. 4, No. 2. - P. 30-37.

J701. Darko Kirovski. Protecting Combinational Logic Synthesis Solutions. / Darko Kirovski, Yean-Yow Hwang, Miodrag Potkonjak, Jason Cong. // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. - 2006. - Vol. 25, No. 12. - P. 2687-2696.

J702. Guishu Liang. Modeling of Transformer Windings Under Very Fast Transient Overvoltages. / Guishu Liang, Haifeng Sun, Xile Zhang, Xiang Cui. // IEEE Transactions on Electromagnetic Compatibility. - 2006. - Vol. 48, No. 4. - P. 621-627.

J703. Solanki K. `Print and Scan' Resilient Data Hiding in Images. / Solanki K., Madhow U., Manjunath B.S., Chandrasekaran S., El-Khalil I. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 4. - P. 464-478.

J704. Zhao H.V. Traitor-Within-Traitor Behavior Forensics: Strategy and Risk Minimization. / Zhao H.V., Liu K.J.R. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 4. - P. 440-456.

J705. Vieira-Marques P.M. Secure Integration of Distributed Medical Data Using Mobile Agents. / Vieira-Marques P.M., Robles S., Cucurull J., Cruz-Correia R.J., Navarro G., Marti R. // IEEE Intelligent Systems. - 2006. - Vol. 21, No. 6. - P. 47-54.

J706. Garfinkel S. Guest Editors' Introduction: Data Surveillance. / Garfinkel S., Smith M.D. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 15-17.

J707. Popp R. Countering Terrorism through Information and Privacy Protection Technologies. / Popp R., Poindexter J. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 18-27.

J708. Hernandez-Guzman Victor. Watermarking Algorithm based on the DWT. / Hernandez-Guzman Victor, Cruz-Ramos Clara, Nakano-Miyatake Mariko, Perez-Meana Hector. // IEEE (Revista IEEE America Latina) Latin America Transactions. - 2006. - Vol. 4, No. 4. - P. 257-267.

J709. Ortega B. News. IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 6-9.

J710. Liebrock L.M. Education: Scholarship for Service. IEEE Distributed Systems Online. - 2006. - Vol. 7, No. 9. - P. 2.

J711. Giakoumaki A. Multiple Image Watermarking Applied to Health Information Management. / Giakoumaki A., Pavlopoulos S., Koutsouris D. // IEEE Transactions on Information Technology in Biomedicine. - 2006. - Vol. 10, No. 4. - P. 722-732.

J712. Daneshgaran F. Iterative joint channel decoding of correlated sources. / Daneshgaran F., Laddomada

M., Mondin M. // IEEE Transactions on Wireless Communications. - 2006. - Vol. 5, No. 10. - P. 2659-2663.

J713. Cupper A. TraX: a device-centric middleware framework for location-based services. / Cupper A., Treu G., Linnhoff-Popien C. // IEEE Communications Magazine. - 2006. - Vol. 44, No. 9. - P. 114-120.

J714. Ketkar A. Nonbinary Stabilizer Codes Over Finite Fields. / Ketkar A., Klappenecker A., Kumar S., Sarvepalli P.K. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 11. - P. 4892-4914.

J715. Adnan Vora. Secure Location Verification Using Radio Broadcast. / Adnan Vora, Mikhail Nesterenko. // IEEE Transactions on Dependable and Secure Computing. - 2006. - Vol. 3, No. 4. - P. 377-385.

J716. Chin-Chen Chang. Reversible Steganography for VQ-Compressed Images Using Side Matching and Relocation. / Chin-Chen Chang, Chih-Yang Lin. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 4. - P. 493-501.

J717. Lee D.C. Some Compartmentalized Secure Task Assignment Models for Distributed Systems. IEEE Transactions on Parallel and Distributed Systems. - 2006. - Vol. 17, No. 12. - P. 1414-1424.

J718. Xiang Pan. Progressive Transmission of Images Over Fading Channels Using Rate-Compatible LDPC Codes. / Xiang Pan, Banihashemi A.H., Cuhadar A. // IEEE Transactions on Image Processing. - 2006. - Vol. 15, No. 12. - P. 3627-3635.

J719. Rubin B.S. Computer Security Education and Research: Handle with Care. / Rubin B.S., Cheung D. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 56-59.

J720. John P. Tomaszewski. Are You Sure You Had a Privacy Incident?. IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 64-66.

J721. Laree Kiely. Systemic Security Management. / Laree Kiely, Terry V. Benzel. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 74-77.

J722. Garfinkel S. Guest Editors' Introduction: Data Surveillance. / Garfinkel S., Smith M.D. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 15-17.

J723. Robert Popp. Countering Terrorism through Information and Privacy Protection Technologies. / Robert Popp, John Poindexter. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 18-27.

J724. William Suchan. Strengthening the Weakest Link in Digital Protection. / William Suchan, Edward Sobiesk. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 78-80.

J725. Shahriar Negahdaripour. An ROV Stereovision System for Ship-Hull Inspection. / Shahriar Negahdaripour, Pezhman Firoozfam. // IEEE Journal of Oceanic Engineering. - 2006. - Vol. 31, No. 3. - P. 551-564.

J726. Rooney Sean. Techniques for integrating sensors into the enterprise network. / Rooney Sean, Bauer Daniel, Scotton Paolo. // IEEE Transactions on Network and Service Management. - 2006. - Vol. 3, No. 1. - P. 43-52.

J727. Qadir M.A. Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents. / Qadir M.A., Ahmad I. // IEEE Aerospace and Electronic Systems Magazine. - 2006. - Vol. 21, No. 11. - P. 18-21.

J728. Sampigethaya K. A Survey on Mix Networks and Their Secure Applications. / Sampigethaya K., Poovendran R. // Proceedings of the IEEE. - 2006. - Vol. 94, No. 12. - P. 2142-2181.

J729. Suchan W. Strengthening the Weakest Link in Digital Protection. / Suchan W., Sobiesk E. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 78-80.

J730. Hegland A.M. A survey of key management in ad hoc networks. / Hegland A.M., Winjum E., Mjolsnes S.F., Rong C., Kure O., Spilling P. // IEEE Communications Surveys & Tutorials. - 2006. - Vol. 8, No. 3. - P. 48-66.

J731. Tomaszewski J.P. Are You Sure You Had a Privacy Incident?. IEEE Security & Privacy. - 2006. - Vol. 4,

No. 6. - P. 64-66.

J732. Kiely L. Systemic Security Management. / Kiely L., Benzel T.V. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 74-77.

J733. {no data available}. News Briefs. IT Professional. - 2006. - Vol. 8, No. 6. - P. 6-11.

J734. {no data available}. News Briefs. IT Professional. - 2006. - Vol. 8, No. 6. - P. 6-11.

J735. Ortega B. News. IEEE Security & Privacy. - 2006. - Vol. 4, No. 6. - P. 6-9.

J736. Wroe A. Silicon Microdosimetry in Heterogeneous Materials: Simulation and Experiment. / Wroe A., Rosenfeld A., Cornelius I., Prokopovich D., Reinhard M., Schulte R., Bashkirov V. // IEEE Transactions on Nuclear Science. - 2006. - Vol. 53, No. 6. - P. 3738-3744.

J737. Williams G. Book Reviews: Breaking Security Design Bottlenecks in Payment Technologies. IEEE Distributed Systems Online. - 2006. - Vol. 7, No. 11. - P. 5.

J738. Tschofenig H. Using SAML to protect the session initiation protocol (SIP). / Tschofenig H., Falk R., Peterson J., Hodges J., Sicker D., Polk J. // IEEE Network. - 2006. - Vol. 20, No. 5. - P. 14-17.

J739. Robbins J. Managing information privacy: developing a context for security and privacy standards convergence. / Robbins J., Sabo J.T. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 4. - P. 92-95.

J740. Ritter T. Integrating Security Policies via Container Portable Interceptors. / Ritter T., Schreiner R., Lang U. // IEEE Distributed Systems Online. - 2006. - Vol. 7, No. 7. - P. 1.

J741. Brooks R.R. Kafka in the academy: a note on ethics in IA education. / Brooks R.R., Vutsinas C. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 4. - P. 50-53.

J742. Trope R.L. Lessons for laptops from the 18th century. / Trope R.L., Power E.M. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 4. - P. 64-68.

J743. Rajagopalan M. System Call Monitoring Using Authenticated System Calls. / Rajagopalan M., Hiltunen M.A., Jim T., Schlichting R.D. // IEEE Transactions on Dependable and Secure Computing. - 2006. - Vol. 3, No. 3. - P. 216-229.

J744. Wen-Nung Lie. Dual protection of JPEG images based on informed embedding and two-stage watermark extraction techniques. / Wen-Nung Lie, Guo-Shiang Lin, Sheng-Lung Cheng. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 3. - P. 330-341.

J745. Harness R.E. For the birds. / Harness R.E., Nielsen L.A. // IEEE Industry Applications Magazine. - 2006. - Vol. 12, No. 4. - P. 38-43.

J746. Mizrak A.T. Detecting and Isolating Malicious Routers. / Mizrak A.T., Yu-Chung Cheng, Marzullo K., Savage S. // IEEE Transactions on Dependable and Secure Computing. - 2006. - Vol. 3, No. 3. - P. 230-244.

J747. Zhao H.V. Behavior forensics for scalable multiuser collusion: fairness versus effectiveness. / Zhao H.V., Liu K.J.R. // IEEE Transactions on Information Forensics and Security. - 2006. - Vol. 1, No. 3. - P. 311-329.

J748. Bo Sun. Enhancing security using mobility-based anomaly detection in cellular mobile networks. / Bo Sun, Fei Yu, Kui Wu, Yang Xiao, Leung V.C.M. // IEEE Transactions on Vehicular Technology. - 2006. - Vol. 55, No. 4. - P. 1385-1396.

J749. Li X.-B. A Tree-Based Data Perturbation Approach for Privacy-Preserving Data Mining. / Li X.-B., Sumit Sarkar. // IEEE Transactions on Knowledge and Data Engineering. - 2006. - Vol. 18, No. 9. - P. 1278-1283.

J750. Chun-Shien Lu. Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection. / Chun-Shien Lu, Shih-Wei Sun, Chao-Yong Hsu, Pao-Chi Chang. // IEEE Transactions on Multimedia. - 2006. - Vol. 8, No. 4. - P. 668-685.

J751. Haohong Wang. Joint source-channel coding for wireless object-based video communications utilizing data hiding. / Haohong Wang, Tsaftaris S.A., Katsaggelos A.K. // IEEE Transactions on Image Processing. -

2006. - Vol. 15, No. 8. - P. 2158-2169.

J752. Gamal H.E. The MIMO ARQ Channel: Diversity–Multiplexing–Delay Tradeoff. / Gamal H.E., Caire G., Damen M.O. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 8. - P. 3601-3621.

J753. Voth D. In the News. IEEE Intelligent Systems. - 2006. - Vol. 21, No. 4. - P. 4-7.

J754. Verdon D. Security policies and the software developer. IEEE Security & Privacy. - 2006. - Vol. 4, No. 4. - P. 42-49.

J755. Junsheng Han. On the Probability of Undetected Error for Overextended Reed–Solomon Codes. / Junsheng Han, Siegel P.H., Lee P. // IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 8. - P. 3662-3669.

J756. Vournas C.D. Postmortem analysis and data validation in the wake of the 2004 Athens blackout. / Vournas C.D., Nikolaidis V.C., Tassoulis A.A. // IEEE Transactions on Power Systems. - 2006. - Vol. 21, No. 3. - P. 1331-1339.

J757. Joshi N. Tamper Proofing by Design Using Generalized Involution-Based Concurrent Error Detection for Involutional Substitution Permutation and Feistel Networks. / Joshi N., Sundararajan J., Wu K., Bo Yang, Karri R. // IEEE Transactions on Computers. - 2006. - Vol. 55, No. 10. - P. 1230-1239.

J758. Phan R.C.-W. A Framework for Describing Block Cipher Cryptanalysis. / Phan R.C.-W., Siddiqi M.U. // IEEE Transactions on Computers. - 2006. - Vol. 55, No. 11. - P. 1402-1409.

J759. Ching-Lai Hor. Unsupervised event extraction within substations using rough classification. / Ching-Lai Hor, Crossley P.A. // IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 4. - P. 1809-1816.

J760. Jacoby G.A. Using Battery Constraints within Mobile Hosts to Improve Network Security. / Jacoby G.A., Marchany R., Davis N. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 5. - P. 40-49.

J761. Montgomery D. Toward Secure Routing Infrastructures. / Montgomery D., Murphy S. // IEEE Security & Privacy. - 2006. - Vol. 4, No. 5. - P. 84-87.

J762. Nath S. A microcomputer-based unique digital fault diagnosis scheme of radial transformer feeders. / Nath S., Chakrabarti A., Mukhopadhyay A.K. // IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 4. - P. 1824-1829.

J763. Dantu R. Securing voice over IP. / Dantu R., Ghosal D., Schulzrinne H. // IEEE Network. - 2006. - Vol. 20, No. 5. - P. 4-5.

J764. Hong Yan. Information leak vulnerabilities in SIP implementations. / Hong Yan, Hui Zhang, Sripanidkulchai K., Zon-Yin Shoe, Saha D. // IEEE Network. - 2006. - Vol. 20, No. 5. - P. 6-13.

J765. Chi-Shan Yu. A discrete Fourier transform-based adaptive mimic phasor estimator for distance relaying applications. IEEE Transactions on Power Delivery. - 2006. - Vol. 21, No. 4. - P. 1836-1846.

J766. Zou C.C. Adaptive Defense Against Various Network Attacks. / Zou C.C., Duffield N., Towsley D., Weibo Gong. // IEEE Journal on Selected Areas in Communications. - 2006. - Vol. 24, No. 10. - P. 1877-1888.

J767. Cunsheng Ding. Complex Codebooks From Combinatorial Designs. IEEE Transactions on Information Theory. - 2006. - Vol. 52, No. 9. - P. 4229-4235.

J768. Hoanca B. Freedom of silence vs. freedom of speech: Technology, law, and information security. IEEE Technology and Society Magazine. - 2006. - Vol. 25, No. 3. - P. 8-15.

J769. Frikken K. Attribute-Based Access Control with Hidden Policies and Hidden Credentials. / Frikken K., Atallah M., Li J. // IEEE Transactions on Computers. - 2006. - Vol. 55, No. 10. - P. 1259-1270.

J770. Ruan X. A New Source Coding Scheme with Small Expected Length and Its Application to Simple Data Encryption. / Ruan X., Katti R.S. // IEEE Transactions on Computers. - 2006. - Vol. 55, No. 10. - P. 1300-1305.

J771. Doerr G. On the Need for Signal-Coherent Watermarks. / Doerr G., Dugelay J.-L., Kirovski D. // IEEE Transactions on Multimedia. - 2006. - Vol. 8, No. 5. - P. 896-904.

J772. Kliewer J. Iterative Source-Channel Decoding With Markov Random Field Source Models. / Kliewer J., Goertz N., Mertins A. // IEEE Transactions on Signal Processing. - 2006. - Vol. 54, No. 10. - P. 3688-3701.

J773. Mills J.E. Cybercrimes against Consumers: Could Biometric Technology Be the Solution?. / Mills J.E., Byun S. // IEEE Internet Computing. - 2006. - Vol. 10, No. 4. - P. 64-71.

J774. Qi Qu. An Adaptive Motion-Based Unequal Error Protection Approach for Real-Time Video Transport Over Wireless IP Networks. / Qi Qu, Yong Pei, Modestino J.W. // IEEE Transactions on Multimedia. - 2006. - Vol. 8, No. 5. - P. 1033-1044.

J775. Rosnes E. On the design of bit-interleaved turbo-coded modulation with low error floors. / Rosnes E., Ytrehus O. // IEEE Transactions on Communications. - 2006. - Vol. 54, No. 9. - P. 1563-1573.

J776. Rabinovitch E. Staying Protected from "Social Engineering". IEEE Communications Magazine. - 2007. - Vol. 45, No. 9. - P. 20-21.

© В.И. Карнышев, 2011
Тематический реферативный сборник сгенерирован в атоматическом режиме
с использованием специализированного программного модуля (ПИО ТУСУР)