Secure computing for java/ dot net

Check following Projects ,also check if any spelling mistakes before showing to your Guide:

1.A simple text-based shoulder surfing resistant graphical password scheme.

Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login.

2. Craigslist Scams and Community Composition: Investigating Online Fraud Victimization.

Synopsis:

Offline, crime and resulting victimization is not individual incidence. It is also hampered or encouraged by the community in which it is situated. Are community characteristics relevant for victimization online? This paper examines the prevalence of Craigslist-based (automobile) scams across 30 American cities. Our methodology analyses historical scam data and its relationship with economic, structural, and cultural characteristics of the communities that are exposed to fraudulent advertising. We find that Craigslist scams are not random, but targeted towards specific communities. The resulting policy insight is for creating public awareness campaigns addressing educated white males, as they are the most vulnerable.

3. A Learning-Based Approach to Reactive Security

Synopsis:

Despite the conventional wisdom that proactive security is superior to reactive security, we show that reactive security can be competitive with proactive security as long as the

reactive defender learns from past attacks instead of myopically overreacting to the last attack. Our game-theoretic model follows common practice in the security literature by making worst case assumptions about the attacker: we grant the attacker complete knowledge of the defender's strategy and do not require the attacker to act rationally. In this model, we bound the competitive ratio between a reactive defense algorithm (which is inspired by online learning theory) and the best fixed proactive defense. Additionally, we show that, unlike proactive defenses, this reactive strategy is robust to a lack of information about the attacker's incentives and knowledge.

4. A Distributed Algorithm for Finding All Best Swap Edges of a Minimum-Diameter Spanning Tree.

Synopsis:

Communication in networks suffers if a link fails. When the links are edges of a tree that has been chosen from an underlying graph of all possible links, a broken link even disconnects the network. Most often, the link is restored rapidly. A good policy to deal with this sort of transient link failures is swap rerouting, where the temporarily broken link is replaced by a single swap link from the underlying graph. A rapid replacement of a broken link by a swap link is only possible if all swap links have been precomputed. The selection of high-quality swap links is essential; it must follow the same objective as the originally chosen communication subnetwork. We are interested in a minimum-diameter tree in a graph with edge weights (so as to minimize the maximum travel time of messages). Hence, each swap link must minimize (among all possible swaps) the diameter of the tree that results from swapping. We propose a distributed algorithm that efficiently computes all of these swap links, and we explain how to route messages across swap edges with a compact routing scheme. Finally, we consider the computation of swap edges in an arbitrary spanning tree, where swap edges are chosen to minimize the time required to adapt routing in case of a failure, and give efficient distributed algorithms for two variants of this problem.

5. Efficiently Outsourcing Multiparty Computation Under Multiple Keys

Synopsis:

Secure multiparty computation enables a set of users to evaluate certain functionalities on their respective inputs while keeping these inputs encrypted throughout the computation. In many applications, however, outsourcing these computations to an untrusted server is desirable, so that the server can perform the computation on behalf of the users. Unfortunately, existing solutions are either inefficient, rely heavily on user interaction, or require the inputs to be encrypted under the same public key - drawbacks making the

employment in practice very limited. We propose a novel technique based on additively homomorphic encryption that avoids all these drawbacks. This method is efficient, requires no user interaction whatsoever (except for data upload and download), and allows evaluating any dynamically chosen function on inputs encrypted under different public keys. Our solution assumes the existence of two non-colluding but untrusted servers that jointly perform the computation by means of a cryptographic protocol. This protocol is proven to be secure in the semi-honest model. By developing application-tailored variants of our approach, we demonstrate its versatility and apply it in two real-world scenarios from different domains, privacy-preserving face recognition and private smart metering. We also give a proof-of-concept implementation to highlight its feasibility.

6. Anomaly Detection via Online Oversampling Principal Component Analysis.

Synopsis:

Anomaly detection has been an important research topic in data mining and machine learning. Many real-world applications such as intrusion or credit card fraud detection require an effective and efficient framework to identify deviated data instances. However, most anomaly detection methods are typically implemented in batch mode, and thus cannot be easily extended to large-scale problems without sacrificing computation and memory requirements. In this paper, we propose an online oversampling principal component analysis (osPCA) algorithm to address this problem, and we aim at detecting the presence of outliers from a large amount of data via an online updating technique. Unlike prior principal component analysis (PCA)-based approaches, we do not store the entire data matrix or covariance matrix, and thus our approach is especially of interest in online or large-scale problems. By oversampling the target instance and extracting the principal direction of the data, the proposed osPCA allows us to determine the anomaly of the target instance according to the variation of the resulting dominant eigenvector. Since our osPCA need not perform eigen analysis explicitly, the proposed framework is favored for online applications which have computation or memory limitations. Compared with the well-known power method for PCA and other popular anomaly detection algorithms, our experimental results verify the feasibility of our proposed method in terms of both accuracy and efficiency.

7. Coding for Cryptographic Security Enhancement Using Stopping Sets.

Synopsis:

In this paper, we discuss the ability of channel codes to enhance cryptographic secrecy. Toward that end, we present the secrecy metric of degrees of freedom in an attacker's

knowledge of the cryptogram, which is similar to equivocation. Using this notion of secrecy, we show how a specific practical channel coding system can be used to hide information about the ciphertext, thus increasing the difficulty of cryptographic attacks. The system setup is the wiretap channel model where transmitted data traverse through independent packet erasure channels (PECs) with public feedback for authenticated automatic repeat-request (ARQ). The code design relies on puncturing nonsystematic low-density parity-check (LDPC) codes with the intent of inflicting an eavesdropper with stopping sets in the decoder. The design amplifies errors when stopping sets occur such that a receiver must guess all the channel-erased bits correctly to avoid an error rate of one half in the ciphertext. We extend previous results on the coding scheme by giving design criteria that reduce the effectiveness of a maximum-likelihood (ML) attack to that of a message-passing (MP) attack. We further extend security analysis to models with multiple receivers and collaborative attackers. Cryptographic security is even enhanced by the system when eavesdroppers have better channel quality than legitimate receivers.

8. Extracting Spread-Spectrum Hidden Data From Digital Media.

Synopsis:

We consider the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video). We develop a novel multicarrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. Experimental studies on images show that the developed algorithm can achieve recovery probability of error close to what may be attained with known embedding carriers and host autocorrelation matrix.

9. Data-Provenance Verification For Secure Hosts.

Synopsis:

Malicious software typically resides stealthily on a user's computer and interacts with the user's computing resources. Our goal in this work is to improve the trustworthiness of a host and its system data. Specifically, we provide a new mechanism that ensures the correct origin or provenance of critical system information and prevents adversaries from utilizing host resources. We define data-provenance integrity as the security property stating that the source where a piece of data is generated cannot be spoofed or tampered with. We describe a cryptographic provenance verification approach for ensuring system properties and

system-data integrity at kernel-level. Its two concrete applications are demonstrated in the keystroke integrity verification and malicious traffic detection. Specifically, we first design and implement an efficient cryptographic protocol that enforces keystroke integrity by utilizing on-chip Trusted Computing Platform (TPM). The protocol prevents the forgery of fake key events by malware under reasonable assumptions. Then, we demonstrate our provenance verification approach by realizing a lightweight framework for restricting outbound malware traffic. This traffic-monitoring framework helps identify network activities of stealthy malware, and lends itself to a powerful personal firewall for examining all outbound traffic of a host that cannot be bypassed.

10. Modeling and Detection of Camouflaging Worm.

Synopsis:

Active worms pose major security threats to the Internet. This is due to the ability of active worms to propagate in an automated fashion as they continuously compromise computers on the Internet. Active worms evolve during their propagation, and thus, pose great challenges to defend against them. In this paper, we investigate a new class of active worms, referred to as Camouflaging Worm (C-Worm in short). The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. Thereby, the C-Worm camouflages its propagation from existing worm detection systems based on analyzing the propagation traffic generated by worms. We analyze characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and nonworm traffic (background traffic). We observe that these two types of traffic are barely distinguishable in the time domain. However, their distinction is clear in the frequency domain, due to the recurring manipulative nature of the C-Worm. Motivated by our observations, we design a novel spectrum-based scheme to detect the C-Worm. Our scheme uses the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to distinguish the C-Worm traffic from background traffic. Using a comprehensive set of detection metrics and real-world traces as background traffic, we conduct extensive performance evaluations on our proposed spectrum-based detection scheme. The performance data clearly demonstrates that our scheme can effectively detect the C-Worm propagation. Furthermore, we show the generality of our spectrum-based scheme in effectively detecting not only the C-Worm, but traditional worms as well.

11. NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems.

Synopsis:

Cloud security is one of most important issues that has attracted a lot of research and development effort in past few years. Particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multistep exploitation, low-frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. This is because cloud users may install vulnerable applications on their virtual machines. To prevent vulnerable virtual machines from being compromised in the cloud, we propose a multiphase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures. The proposed framework leverages OpenFlow network programming APIs to build a monitor and control plane over distributed programmable virtual switches to significantly improve attack detection and mitigate attack consequences. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

12. Detecting Anomalous Insiders in Collaborative Information Systems.

Synopsis:

Collaborative information systems (CISs) are deployed within a diverse array of environments that manage sensitive information. Current security mechanisms detect insider threats, but they are ill-suited to monitor systems in which users function in dynamic teams. In this paper, we introduce the community anomaly detection system (CADS), an unsupervised learning framework to detect insider threats based on the access logs of collaborative environments. The framework is based on the observation that typical CIS users tend to form community structures based on the subjects accessed (e.g., patients' records viewed by healthcare providers). CADS consists of two components: 1) relational pattern extraction, which derives community structures and 2) anomaly prediction, which leverages a statistical model to determine when users have sufficiently deviated from communities. We further extend CADS into MetaCADS to account for the semantics of subjects (e.g., patients' diagnoses). To empirically evaluate the framework, we perform an assessment with three months of access logs from a real electronic health record (EHR) system in a large medical center. The results illustrate our models exhibit significant performance gains over state-of-the-art competitors. When the number of illicit users is low, MetaCADS is the best model, but as the number grows, commonly accessed semantics lead to hiding in a crowd, such that CADS is more prudent.

13. Nymble: Blocking Misbehaving Users in Anonymizing Networks.

Synopsis:

Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular Web sites. Web site administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem, we present Nymble, a system in which servers can “blacklist” misbehaving users, thereby blocking users without compromising their anonymity. Our system is thus agnostic to different servers' definitions of misbehavior-servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

14. On Inference-Proof View Processing of XML Documents.

Synopsis:

This work aims at treating the inference problem in XML documents that are assumed to represent potentially incomplete information. The inference problem consists in providing a control mechanism for enforcing inference-usability confinement of XML documents. More formally, an inference-proof view of an XML document is required to be both indistinguishable from the actual XML document to the clients under their inference capabilities, and to neither contain nor imply any confidential information. We present an algorithm for generating an inference-proof view by weakening the actual XML document, i.e., eliminating confidential information and other information that could be used to infer confidential information. In order to avoid inferences based on the schema of the XML documents, the DTD of the actual XML document is modified according to the weakening operations as well, such that the modified DTD conforms with the generated inference-proof view.

15. Detecting Spam Zombies by Monitoring Outgoing Messages.

Synopsis:

Compromised machines are one of the key security threats on the Internet; they are often used to launch various security attacks such as spamming and spreading malware, DDoS, and identity theft. Given that spamming provides a key economic incentive for attackers to recruit the large number of compromised machines, we focus on the detection of the compromised machines in a network that are involved in the spamming activities, commonly known as spam zombies. We develop an effective spam zombie detection system named SPOT by monitoring outgoing messages of a network. SPOT is designed based on a powerful statistical tool called Sequential Probability Ratio Test, which has bounded false positive and false negative error rates. In addition, we also evaluate the performance of the developed SPOT system using a two-month e-mail trace collected in a large US campus network. Our evaluation studies show that SPOT is an effective and efficient system in automatically detecting compromised machines in a network. For example, among the 440 internal IP addresses observed in the e-mail trace, SPOT identifies 132 of them as being associated with compromised machines. Out of the 132 IP addresses identified by SPOT, 126 can be either independently confirmed (110) or highly likely (16) to be compromised. Moreover, only seven internal IP addresses associated with compromised machines in the trace are missed by SPOT. In addition, we also compare the performance of SPOT with two other spam zombie detection algorithms based on the number and percentage of spam messages originated or forwarded by internal machines, respectively, and show that SPOT outperforms these two detection algorithms.

16. PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance.

Synopsis:

Pay-As-You-Drive insurance schemes are establishing themselves as the future of car insurance. However, their current implementations, in which fine-grained location data are sent to insurers, entail a serious privacy risk. We present PriPAYD, a system where the premium calculations are performed locally in the vehicle, and only aggregated data are sent to the insurance company, without leaking location information. Our design is based on well-understood security techniques that ensure its correct functioning. We discuss the viability of PriPAYD in terms of cost, security, and ease of certification. We demonstrate that PriPAYD is possible through a proof-of-concept implementation that shows how privacy can be obtained at a very reasonable extra cost.

17. Privacy Preserving Data Analytics for Smart Homes.

Synopsis:

A framework for maintaining security & preserving privacy for analysis of sensor data from smart homes, without compromising on data utility is presented. Storing the personally identifiable data as hashed values withholds identifiable information from any computing nodes. However the very nature of smart home data analytics is establishing preventive care. Data processing results should be identifiable to certain users responsible for direct care. Through a separate encrypted identifier dictionary with hashed and actual values of all unique sets of identifiers, we suggest re-identification of any data processing results. However the level of re-identification needs to be controlled, depending on the type of user accessing the results. Generalization and suppression on identifiers from the identifier dictionary before re-introduction could achieve different levels of privacy preservation. In this paper we propose an approach to achieve data security & privacy through out the complete data lifecycle: data generation/collection, transfer, storage, processing and sharing.

18. Secure Encounter-Based Mobile Social Networks: Requirements, Designs, and Tradeoffs.

Encounter-based social networks and encounter-based systems link users who share a location at the same time, as opposed to the traditional social network paradigm of linking users who have an offline friendship. This new approach presents challenges that are fundamentally different from those tackled by previous social network designs. In this paper, we explore the functional and security requirements for these new systems, such as availability, security, and privacy, and present several design options for building secure encounter-based social networks. To highlight these challenges, we examine one recently proposed encounter-based social network design and compare it to a set of idealized security and functionality requirements. We show that it is vulnerable to several attacks, including impersonation, collusion, and privacy breaching, even though it was designed specifically for security. Mindful of the possible pitfalls, we construct a flexible framework for secure encounter-based social networks, which can be used to construct networks that offer different security, privacy, and availability guarantees. We describe two example constructions derived from this framework, and consider each in terms of the ideal requirements. Some of our new designs fulfill more requirements in terms of system security, reliability, and privacy than previous work. We also evaluate real-world performance of one of our designs by implementing a proof-of-concept iPhone application called MeetUp. Experiments highlight the potential of our system and hint at the deployability of our designs on a large scale.

19. A Methodology for Direct and Indirect Discrimination Prevention in Data Mining.

Synopsis:

Data mining is an increasingly important technology for extracting useful knowledge hidden in large collections of data. There are, however, negative social perceptions about data mining, among which potential privacy invasion and potential discrimination. The latter consists of unfairly treating people on the basis of their belonging to a specific group. Automated data collection and data mining techniques such as classification rule mining have paved the way to making automated decisions, like loan granting/denial, insurance premium computation, etc. If the training data sets are biased in what regards discriminatory (sensitive) attributes like gender, race, religion, etc., discriminatory decisions may ensue. For this reason, anti-discrimination techniques including discrimination discovery and prevention have been introduced in data mining. Discrimination can be either direct or indirect. Direct discrimination occurs when decisions are made based on sensitive attributes. Indirect discrimination occurs when decisions are made based on nonsensitive attributes which are strongly correlated with biased sensitive ones. In this paper, we tackle discrimination prevention in data mining and propose new techniques applicable for direct or indirect discrimination prevention individually or both at the same time. We discuss how to clean training data sets and outsourced data sets in such a way that direct and/or indirect discriminatory decision rules are converted to legitimate (nondiscriminatory) classification rules. We also propose new metrics to evaluate the utility of the proposed approaches and we compare these approaches. The experimental evaluations demonstrate that the proposed techniques are effective at removing direct and/or indirect discrimination biases in the original data set while preserving data quality.

20. DoubleGuard: Detecting Intrusions in Multitier Web Applications.

Synopsis:

Internet services and applications have become an inextricable part of daily life, enabling communication and the management of personal information from anywhere. To accommodate this increase in application and data complexity, web services have moved to a multitiered design wherein the webserver runs the application front-end logic and data are outsourced to a database or file server. In this paper, we present DoubleGuard, an IDS system that models the network behavior of user sessions across both the front-end webserver and the back-end database. By monitoring both web and subsequent database requests, we are able to ferret out attacks that an independent IDS would not be able to identify. Furthermore, we quantify the limitations of any multitier IDS in terms of training

sessions and functionality coverage. We implemented DoubleGuard using an Apache webserver with MySQL and lightweight virtualization. We then collected and processed real-world traffic over a 15-day period of system deployment in both dynamic and static web applications. Finally, using DoubleGuard, we were able to expose a wide range of attacks with 100 percent accuracy while maintaining 0 percent false positives for static web services and 0.6 percent false positives for dynamic web services.

21. RITAS: Services for Randomized Intrusion Tolerance.

Synopsis:

Randomized agreement protocols have been around for more than two decades. Often assumed to be inefficient due to their high expected communication and computation complexities, they have remained overlooked by the community-at-large as a valid solution for the deployment of fault-tolerant distributed systems. This paper aims to demonstrate that randomization can be a very competitive approach even in hostile environments where arbitrary faults can occur. A stack of randomized intrusion-tolerant protocols is described and its performance evaluated under several settings in both local-area-network (LAN) and wide-area-network environments. The stack provides a set of relevant services ranging from basic communication primitives up to atomic broadcast. The experimental evaluation shows that the protocols are efficient, especially in LAN environments where no performance reduction is observed under certain Byzantine faults.

22. SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks.

Synopsis:

Anonymity has received increasing attention in the literature due to the users' awareness of their privacy nowadays. Anonymity provides protection for users to enjoy network services without being traced. While anonymity-related issues have been extensively studied in payment-based systems such as e-cash and peer-to-peer (P2P) systems, little effort has been devoted to wireless mesh networks (WMNs). On the other hand, the network authority requires conditional anonymity such that misbehaving entities in the network remain traceable. In this paper, we propose a security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. The proposed architecture strives to resolve the conflicts between the anonymity and traceability objectives, in addition to guaranteeing fundamental security requirements including authentication, confidentiality, data integrity, and nonrepudiation. Thorough analysis on security and efficiency is incorporated, demonstrating the feasibility and effectiveness of the proposed architecture.

23. Securing Online Reputation Systems Through Trust Modeling and Temporal Analysis.

Synopsis:

With the rapid development of reputation systems in various online social networks, manipulations against such systems are evolving quickly. In this paper, we propose scheme TATA, the abbreviation of joint Temporal And Trust Analysis, which protects reputation systems from a new angle: the combination of time domain anomaly detection and Dempster-Shafer theory-based trust computation. Real user attack data collected from a cyber competition is used to construct the testing data set. Compared with two representative reputation schemes and our previous scheme, TATA achieves a significantly better performance in terms of identifying items under attack, detecting malicious users who insert dishonest ratings, and recovering reputation scores.

24. Securing Online Reputation Systems Through Trust Modeling and Temporal Analysis.

Synopsis:

With the rapid development of reputation systems in various online social networks, manipulations against such systems are evolving quickly. In this paper, we propose scheme TATA, the abbreviation of joint Temporal And Trust Analysis, which protects reputation systems from a new angle: the combination of time domain anomaly detection and Dempster-Shafer theory-based trust computation. Real user attack data collected from a cyber competition is used to construct the testing data set. Compared with two representative reputation schemes and our previous scheme, TATA achieves a significantly better performance in terms of identifying items under attack, detecting malicious users who insert dishonest ratings, and recovering reputation scores.

25. Ensuring Distributed Accountability for Data Sharing in the Cloud.

Synopsis:

Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the

wide adoption of cloud services. To address this problem, in this paper, we propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, we propose an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. We leverage the JAR programmable capabilities to both create a dynamic and traveling object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, we also provide distributed auditing mechanisms. We provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.

26. Secure Overlay Cloud Storage with Access Control and Assured Deletion.

Synopsis:

We can now outsource data backups off-site to third-party cloud storage services so as to reduce data management costs. However, we must provide security guarantees for the outsourced data, which is now maintained by third parties. We design and implement FADE, a secure overlay cloud storage system that achieves fine-grained, policy-based access control and file assured deletion. It associates outsourced files with file access policies, and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. To achieve such security goals, FADE is built upon a set of cryptographic key operations that are self-maintained by a quorum of key managers that are independent of third-party clouds. In particular, FADE acts as an overlay system that works seamlessly atop today's cloud storage services. We implement a proof-of-concept prototype of FADE atop Amazon S3, one of today's cloud storage services. We conduct extensive empirical studies, and demonstrate that FADE provides security protection for outsourced data, while introducing only minimal performance and monetary cost overhead. Our work provides insights of how to incorporate value-added security features into today's cloud storage services.

27. Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks.

Synopsis:

Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In this paper, however, we demonstrative that their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, we present two impersonation attacks. The first attack allows a malicious service provider, who has successfully communicated with a legal user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In another attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang-Lee scheme. Moreover, by employing an efficient verifiable encryption of RSA signatures proposed by Ateniese, we propose an improvement for repairing the Chang-Lee scheme. We promote the formal study of the soundness of authentication as one open problem.

28. Security and Privacy-Enhancing Multicloud Architectures.

Synopsis:

Security challenges are still among the biggest obstacles when considering the adoption of cloud services. This triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues, the cloud paradigm comes with a new set of unique features, which open the path toward novel security approaches, techniques, and architectures. This paper provides a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects.

29. Security using colors and Armstrong numbers.

Synopsis:

In real world, data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. The universal technique for providing confidentiality of transmitted data is cryptography. This paper provides a technique to encrypt the data using a key involving Armstrong numbers and colors as the password. Three set of keys are used to provide secure data transmission with the colors acting as vital security element thereby providing authentication.

30. SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems.

Synopsis:

Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. This paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust, service, and recommendation contexts, are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on 16 different malicious behavior models. In the experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers.

31. Fast and Accurate Annotation of Short Texts with Wikipedia Pages.

Synopsis:

Several recent software systems have been designed to obtain novel annotation of cross-referencing text fragments and Wikipedia pages. Tagme is state of the art in this setting and can accurately manage short textual fragments (such as snippets of search engine results, tweets, news, or blogs) on the fly.

32. Online Modeling of Proactive Moderation System for Auction Fraud Detection.

Synopsis:

We consider the problem of building online machine-learned models for detecting auction frauds in e-commence web sites. Since the emergence of the world wide web, online shopping and online auction have gained more and more popularity. While people are enjoying the benefits from online trading, criminals are also taking advantages to conduct fraudulent activities against honest parties to obtain illegal profit. Hence proactive fraud-detection moderation systems are commonly applied in practice to detect and prevent such illegal and fraud activities. Machine-learned models, especially those that are learned online, are able to catch frauds more efficiently and quickly than human-tuned rule-based systems. In this paper, we propose an online probit model framework which takes online feature selection, coefficient bounds from human knowledge and multiple instance learning into account simultaneously. By empirical experiments on a real-world online auction fraud detection data we show that this model can potentially detect more frauds and significantly reduce customer complaints compared to several baseline models and the human-tuned rule-based system.

33. Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data.

Synopsis:

Cloud computing has emerging as a promising pattern for data outsourcing and high-quality data services. However, concerns of sensitive information on cloud potentially causes privacy problems. Data encryption protects data security to some extent, but at the cost of compromised efficiency. Searchable symmetric encryption (SSE) allows retrieval of encrypted data over cloud. In this paper, we focus on addressing data privacy issues using SSE. For the first time, we formulate the privacy issue from the aspect of similarity relevance and scheme robustness. We observe that server-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a two-round searchable encryption (TRSE) scheme that supports top-k multikeyword retrieval. In TRSE, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext. As a result, information leakage can be eliminated and data security is ensured. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency.

34. TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing.

Synopsis:

The ubiquity of the various cheap embedded sensors on mobile devices, for example cameras, microphones, accelerometers, and so on, is enabling the emergence of participatory sensing applications. While participatory sensing can benefit the individuals and communities greatly, the collection and analysis of the participators' location and trajectory data may jeopardize their privacy. However, the existing proposals mostly focus on participators' location privacy, and few are done on participators' trajectory privacy. The effective analysis on trajectories that contain spatial-temporal history information will reveal participators' whereabouts and the relevant personal privacy. In this paper, we propose a trajectory privacy-preserving framework, named TrPF, for participatory sensing. Based on the framework, we improve the theoretical mix-zones model with considering the time factor from the perspective of graph theory. Finally, we analyze the threat models with different background knowledge and evaluate the effectiveness of our proposal on the basis of information entropy, and then compare the performance of our proposal with previous trajectory privacy protections. The analysis and simulation results prove that our proposal can protect participators' trajectories privacy effectively with lower information loss and costs than what is afforded by the other proposals.

35. Packet-Hiding Methods for Preventing Selective Jamming Attacks.

Synopsis:

The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launchpad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.

36. pCloud: A Distributed System for Practical PIR.

Synopsis:

Computational Private Information Retrieval (cPIR) protocols allow a client to retrieve one bit from a database, without the server inferring any information about the queried bit. These protocols are too costly in practice because they invoke complex arithmetic operations for every bit of the database. In this paper, we present pCloud, a distributed system that constitutes the first attempt toward practical cPIR. Our approach assumes a disk-based architecture that retrieves one page with a single query. Using a striping technique, we distribute the database to a number of cooperative peers, and leverage their computational resources to process cPIR queries in parallel. We implemented pCloud on the PlanetLab network, and experimented extensively with several system parameters. Our results indicate that pCloud reduces considerably the query response time compared to the traditional client/server model, and has a very low communication overhead. Additionally, it scales well with an increasing number of peers, achieving a linear speedup.

37. Two tales of privacy in online social networks.

Synopsis:

Privacy is one of the friction points that emerge when communications are mediated in online social networks (OSNs). Different communities of computer science researchers have framed the OSN privacy problem as one of surveillance, institutional privacy, or social privacy. In tackling these problems, researchers have also treated them as if they were independent. In this article, the authors argue that the different privacy problems are entangled and that OSN privacy research would benefit from a more holistic approach.

38. Utility-Privacy Tradeoffs in Databases: An Information-Theoretic Approach.

Synopsis:

Ensuring the usefulness of electronic data sources while providing necessary privacy guarantees is an important unsolved problem. This problem drives the need for an analytical framework that can quantify the privacy of personally identifiable information while still providing a quantifiable benefit (utility) to multiple legitimate information consumers. This paper presents an information-theoretic framework that promises an analytical model guaranteeing tight bounds of how much utility is possible for a given level of privacy and vice-versa. Specific contributions include: 1) stochastic data models for both categorical and numerical data; 2) utility-privacy tradeoff regions and the encoding (sanization) schemes achieving them for both classes and their practical relevance; and 3) modeling of prior knowledge at the user and/or data source and optimal encoding schemes for both cases.

39. Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism.

Synopsis:

This paper presents an integrated evaluation of the Persuasive Cued Click-Points graphical password scheme, including usability and security evaluations, and implementation considerations. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points.

40. Privacy-Preserving Enforcement of Spatially Aware RBAC.

Synopsis:

Several models for incorporating spatial constraints into role-based access control (RBAC) have been proposed, and researchers are now focusing on the challenge of ensuring such policies are enforced correctly. However, existing approaches have a major shortcoming, as they assume the server is trustworthy and require complete disclosure of sensitive location information by the user. In this work, we propose a novel framework and a set of protocols to solve this problem. Specifically, in our scheme, a user provides a service provider with role and location tokens along with a request. The service provider consults with a role authority and a location authority to verify the tokens and evaluate the policy. However, none of the servers learn the requesting user's identity, role, or location. In this paper, we define the protocols and the policy enforcement scheme, and present a formal proof of a number of security properties..

41. Remote Attestation with Domain-Based Integrity Model and Policy Analysis.

Synopsis:

We propose and implement an innovative remote attestation framework called DR@FT for efficiently measuring a target system based on an information flow-based integrity model. With this model, the high integrity processes of a system are first measured and verified, and these

processes are then protected from accesses initiated by low integrity processes. Toward dynamic systems with frequently changed system states, our framework verifies the latest state changes of a target system instead of considering the entire system information. Our attestation evaluation adopts a graph-based method to represent integrity violations, and the graph-based policy analysis is further augmented with a ranked violation graph to support high semantic reasoning of attestation results. As a result, DR@FT provides efficient and effective attestation of a system's integrity status, and offers intuitive reasoning of attestation results for security administrators. Our experimental results demonstrate the feasibility and practicality of DR@FT.

42. Risk-Aware Mitigation for MANET Routing Attacks.

Synopsis:

Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. Even though there exist several intrusion response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naïve fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naïve fuzzy responses could lead to uncertainty in countering routing attacks in MANET. In this paper, we propose a risk-aware response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of several performance metrics.

43. Secure Overlay Cloud Storage with Access Control and Assured Deletion.

Synopsis:

We can now outsource data backups off-site to third-party cloud storage services so as to reduce data management costs. However, we must provide security guarantees for the outsourced data, which is now maintained by third parties. We design and implement FADE, a secure overlay cloud storage system that achieves fine-grained, policy-based access control and file assured deletion. It associates outsourced files with file access policies, and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. To achieve such security goals, FADE is built upon a set of cryptographic key operations that are self-maintained by a quorum of key managers that are independent of third-party clouds. In particular, FADE acts as an overlay system that works seamlessly atop today's cloud storage services. We implement a proof-of-concept

prototype of FADE atop Amazon S3, one of today's cloud storage services. We conduct extensive empirical studies, and demonstrate that FADE provides security protection for outsourced data, while introducing only minimal performance and monetary cost overhead. Our work provides insights of how to incorporate value-added security features into today's cloud storage services.

44. SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems

Synopsis:

Security and privacy issues have become critically important with the fast expansion of multiagent systems. Most network applications such as pervasive computing, grid computing, and P2P networks can be viewed as multiagent systems which are open, anonymous, and dynamic in nature. Such characteristics of multiagent systems introduce vulnerabilities and threats to providing secured communication. One feasible way to minimize the threats is to evaluate the trust and reputation of the interacting agents. Many trust/reputation models have done so, but they fail to properly evaluate trust when malicious agents start to behave in an unpredictable way. Moreover, these models are ineffective in providing quick response to a malicious agent's oscillating behavior. Another aspect of multiagent systems which is becoming critical for sustaining good service quality is the even distribution of workload among service providing agents. Most trust/reputation models have not yet addressed this issue. So, to cope with the strategically altering behavior of malicious agents and to distribute workload as evenly as possible among service providers; we present in this paper a dynamic trust computation model called "SecuredTrust.” In this paper, we first analyze the different factors related to evaluating the trust of an agent and then propose a comprehensive quantitative model for measuring such trust. We also propose a novel load-balancing algorithm based on the different factors defined in our model. Simulation results indicate that our model compared to other existing models can effectively cope with strategic behavioral change of malicious agents and at the same time efficiently distribute workload among the service providing agents under stable condition.

45. Security architecture for cloud networking.

Synopsis:

Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). A new approach called cloud networking adds networking functionalities to cloud computing and enables dynamic and flexible placement of virtual resources crossing provider borders. This allows various kinds of optimization,

e.g., reducing latency or network load. However, this approach introduces new security challenges. This paper presents a security architecture that enables a user of cloud networking to define security requirements and enforce them in the cloud networking infrastructure.

46. Defending against Web Application Vulnerabilities.

Synopsis:

Although no single tool or technique can guard against the host of possible attacks, a defense-in-depth approach, with overlapping protections, can help secure Web applications.

47. CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring.

Synopsis:

Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to address this important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy reencryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

48. An efficient and provably-secure coercion-resistant e-voting protocol.

We present an efficient and provably-secure e-voting protocol, which is a variant of the JCJ e-voting protocol (Juels et al., 2010). It decreases the total number of JCJ's operations from O(n2) to O(n), where n is the number of votes or voters (whichever is the maximum). Note that since the operations under consideration are time-consuming (e.g., public-key encryption), the improvement is quite substantial. As a rough comparison, consider a nation-wide election with around ten million voters/votes. Assuming each operation takes one microsecond, and no parallelization is used, one can see a huge difference: our

protocol tallies the votes in 10 seconds, while the JCJ protocol requires over 3 years to tally the votes. In order to achieve this level of efficiency, we change the ballot format and the tallying phase of the JCJ protocol. Moreover, we provide a complexity analysis and a detailed proof for coercion-resistance of our protocol.

49. A Novel Data Embedding Method Using Adaptive Pixel Pair Matching.

Synopsis:

This paper proposes a new data-hiding method based on pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. Exploiting modification direction (EMD) and diamond encoding (DE) are two data-hiding methods proposed recently based on PPM. The maximum capacity of EMD is 1.161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads. Experimental results reveal that the proposed method not only provides better performance than those of OPAP and DE, but also is secure under the detection of some well-known steganalysis techniques.

50. A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group.

Synopsis:

The (t, n) visual cryptography (VC) is a secret sharing scheme where a secret image is encoded into n transparencies, and the stacking of any t out of n transparencies reveals the secret image. The stacking of t - 1 or fewer transparencies is unable to extract any information about the secret. We discuss the additions and deletions of users in a dynamic user group. To reduce the overhead of generating and distributing transparencies in user changes, this paper proposes a (t, n) VC scheme with unlimited n based on the probabilistic model. The proposed scheme allows n to change dynamically in order to include new transparencies without regenerating and redistributing the original transparencies. Specifically, an extended VC scheme based on basis matrices and a probabilistic model is proposed. An equation is derived from the fundamental definitions of the (t, n) VC scheme, and then the (t, ∞) VC scheme achieving maximal contrast can be designed by using the derived equation. The maximal contrasts with t = 2 to 6 are explicitly solved in this paper.

51. A Policy Enforcing Mechanism for Trusted Ad Hoc Networks.

Synopsis:

To ensure fair and secure communication in Mobile Ad hoc Networks (MANETs), the applications running in these networks must be regulated by proper communication policies. However, enforcing policies in MANETs is challenging because they lack the infrastructure and trusted entities encountered in traditional distributed systems. This paper presents the design and implementation of a policy enforcing mechanism based on Satem, a kernel-level trusted execution monitor built on top of the Trusted Platform Module. Under this mechanism, each application or protocol has an associated policy. Two instances of an application running on different nodes may engage in communication only if these nodes enforce the same set of policies for both the application and the underlying protocols used by the application. In this way, nodes can form trusted application-centric networks. Before allowing a node to join such a network, Satem verifies its trustworthiness of enforcing the required set of policies. Furthermore, Satem protects the policies and the software enforcing these policies from being tampered with. If any of them is compromised, Satem disconnects the node from the network. We demonstrate the correctness of our solution through security analysis, and its low overhead through performance evaluation of two MANET applications.

52. Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing.

Synopsis:

Today's organizations raise an increasing need for information sharing via on-demand access. Information brokering systems (IBSs) have been proposed to connect large-scale loosely federated data sources via a brokering overlay, in which the brokers make routing decisions to direct client queries to the requested data servers. Many existing IBSs assume that brokers are trusted and thus only adopt server-side access control for data confidentiality. However, privacy of data location and data consumer can still be inferred from metadata (such as query and access control rules) exchanged within the IBS, but little attention has been put on its protection. In this paper, we propose a novel approach to preserve privacy of multiple stakeholders involved in the information brokering process. We are among the first to formally define two privacy attacks, namely attribute-correlation attack and inference attack, and propose two countermeasure schemes automaton segmentation and query segment encryption to securely share the routing decision-making responsibility among a selected set of brokering servers. With comprehensive security analysis and experimental results, we show that our approach seamlessly integrates security enforcement with query routing to provide system-wide security with insignificant overhead.

53. Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks.

Synopsis:

Data sensing and retrieval in wireless sensor systems have a widespread application in areas such as security and surveillance monitoring, and command and control in battlefields. In query-based wireless sensor systems, a user would issue a query and expect a response to be returned within the deadline. While the use of fault tolerance mechanisms through redundancy improves query reliability in the presence of unreliable wireless communication and sensor faults, it could cause the energy of the system to be quickly depleted. Therefore, there is an inherent trade-off between query reliability versus energy consumption in query-based wireless sensor systems. In this paper, we develop adaptive fault-tolerant quality of service (QoS) control algorithms based on hop-by-hop data delivery utilizing “source” and “path” redundancy, with the goal to satisfy application QoS requirements while prolonging the lifetime of the sensor system. We develop a mathematical model for the lifetime of the sensor system as a function of system parameters including the “source” and “path” redundancy levels utilized. We discover that there exists optimal “source” and “path” redundancy under which the lifetime of the system is maximized while satisfying application QoS requirements. Numerical data are presented and validated through extensive simulation, with physical interpretations given, to demonstrate the feasibility of our algorithm design.

54. Access control for online social networks third party application.

Synopsis:

With the development of Web 2.0 technologies, online social networks are able to provide open platforms to enable the seamless sharing of profile data to enable public developers to interface and extend the social network services as applications. At the same time, these open interfaces pose serious privacy concerns as third party applications are usually given access to the user profiles. Current related research has focused on mainly user-to-user interactions in social networks, and seems to ignore the third party applications. In this paper, we present an access control framework to manage third party applications. Our framework is based on enabling the user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes. We model applications as finite state machines, and use the required user profile attributes as conditions governing the application execution. We formulate the minimal

attribute generalization problem and we propose a solution that maps the problem to the shortest path problem to find the minimum set of attribute generalization required to access the application services. We assess the feasibility of our approach by developing a proof-of-concept implementation and by conducting user studies on a widely-used social network platform.

55. Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error.

Synopsis:

This paper deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis, we target the motion vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The choice of candidate subset of these motion vectors are based on their associated macroblock prediction error, which is different from the approaches based on the motion vector attributes such as the magnitude and phase angle, etc. A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level. The secret message bitstream is embedded in the least significant bit of both components of the candidate motion vectors. The method is implemented and tested for hiding data in natural sequences of multiple groups of pictures and the results are evaluated. The evaluation is based on two criteria: minimum distortion to the reconstructed video and minimum overhead on the compressed video size. Based on the aforementioned criteria, the proposed method is found to perform well and is compared to a motion vector attribute-based method from the literature.

56. Non-Cooperative Location Privacy

Synopsis:

In mobile networks, authentication is a required primitive for most security protocols. Unfortunately, an adversary can monitor pseudonyms used for authentication to track the location of mobile nodes. A frequently proposed solution to protect location privacy suggests that mobile nodes collectively change their pseudonyms in regions called mix zones. This approach is costly. Self-interested mobile nodes might, thus, decide not to cooperate and jeopardize the achievable location privacy. In this paper, we analyze non-cooperative behavior of mobile nodes by using a game-theoretic model, where each player aims at maximizing its location

privacy at a minimum cost. We obtain Nash equilibria in static n-player complete information games. As in practice mobile nodes do not know their opponents' payoffs, we then consider static incomplete information games. We establish that symmetric Bayesian-Nash equilibria exist with simple threshold strategies. By means of numerical results, we predict behavior of selfish mobile nodes. We then investigate dynamic games where players decide to change their pseudonym one after the other and show how this affects strategies at equilibrium. Finally, we design protocols-PseudoGame protocols-based on the results of our analysis and simulate their performance in vehicular network scenarios.

57. Improving Security and Performance in the Tor Network through Tunable Path Selection.

Synopsis:

The Tor anonymous communication network uses self-reported bandwidth values to select routers for building tunnels. Since tunnels are allocated in proportion to this bandwidth, this allows a malicious router operator to attract tunnels for compromise. Although Tor limits the self-reported bandwidth, it uses a high maximum value, effectively choosing performance over high anonymity for all users. We propose a router selection algorithm that allows users to control the trade-off between performance and anonymity. We also propose an opportunistic bandwidth measurement algorithm to replace self-reported values that is more sensitive to load and more responsive to changing network conditions. Our mechanism effectively blends the traffic from users of different preferences, making partitioning attacks difficult. We implemented the opportunistic measurement and tunable performance extensions and examined their performance both through simulation and in the real Tor network. Our results show that users can get dramatic increases in either performance or anonymity with little to no sacrifice in the other metric, or a more modest improvement in both. Our mechanisms are also invulnerable to the previously published low-resource attacks on Tor.

58. An Approach to Detect and Prevent Tautology Type SQL Injection in Web Service Based on XSchema validation.

Synopsis:

SQL injection is the most common attack for web applications and widely used attacking method by hackers all over the world.

This is an attacking method that aims the data stored in a database through the firewall that shield it. The poor input validation in code and

website administration leads SQL injection to attack the web resource. This proposed system exhibit a dynamic method to detect and prevent

tautology type SQL Injection from malicious web users who wants to access any resource in web related application. To detect malicious

attack and prevent malicious users from accessing web resources, this system uses an effective SQL Query processing based on XML

Schema validation. This proposed system can be used in web application logging and security. This work also concludes effectiveness and

performance of the system using the resultant data of proposed system..

59. IPAS: Implicit Password Authentication System.

Synopsis:

Authentication is the first line of defense against compromising confidentiality and integrity. Though traditional login/password based schemes are easy to implement, they have been subjected to several attacks. As an alternative, token and biometric based authentication systems were introduced. However, they have not improved substantially to justify the investment. Thus, a variation to the login/password scheme, viz. graphical scheme was introduced. But it also suffered due to shoulder-surfing and screen dump attacks. In this paper, we introduce a framework of our proposed (IPAS) Implicit Password Authentication System, which is immune to the common attacks suffered by other authentication schemes.

60. Privacy Preserving Data Sharing With Anonymous ID Assignment.

Synopsis:

An algorithm for anonymous sharing of private data among parties is developed. This technique is used iteratively to assign these nodes ID numbers ranging from 1 to . This assignment is anonymous in that the identities received are unknown to the other members of the group.

Resistance to collusion among other members is verified in an information theoretic sense when private communication channels are used. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining, collision avoidance in communications and distributed database access. The required computations are distributed without using a trusted central authority. Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements. The new algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for distributed solution of certain polynomials over finite fields enhances the scalability of the algorithms. Markov chain representations are used to find statistics on the number of iterations required, and computer algebra gives closed form results for the completion rates.

61. Online Intrusion Alert Aggregation with Generative Data Stream Modeling.

Synopsis:

Alert aggregation is an important subtask of intrusion detection. The goal is to identify and to cluster different alerts-produced by low-level intrusion detection systems, firewalls, etc.-belonging to a specific attack instance which has been initiated by an attacker at a certain point in time. Thus, meta-alerts can be generated for the clusters that contain all the relevant information whereas the amount of data (i.e., alerts) can be reduced substantially. Meta-alerts may then be the basis for reporting to security experts or for communication within a distributed intrusion detection system. We propose a novel technique for online alert aggregation which is based on a dynamic, probabilistic model of the current attack situation. Basically, it can be regarded as a data stream version of a maximum likelihood approach for the estimation of the model parameters. With three benchmark data sets, we demonstrate that it is possible to achieve reduction rates of up to 99.96 percent while the number of missing meta-alerts is extremely low. In addition, meta-alerts are generated with a delay of typically only a few seconds after observing the first alert belonging to a new attack instance.

62. Automatic Reconfiguration for Large-Scale Reliable Storage Systems.

Synopsis:

Byzantine-fault-tolerant replication enhances the availability and reliability of Internet services that store critical state and preserve it despite attacks or software errors. However, existing Byzantine-fault-tolerant storage systems either assume a static set of replicas, or have limitations in how they handle reconfigurations (e.g., in terms of the scalability of the

solutions or the consistency levels they provide). This can be problematic in long-lived, large-scale systems where system membership is likely to change during the system lifetime. In this paper, we present a complete solution for dynamically changing system membership in a large-scale Byzantine-fault-tolerant system. We present a service that tracks system membership and periodically notifies other system nodes of membership changes. The membership service runs mostly automatically, to avoid human configuration errors; is itself Byzantine-fault-tolerant and reconfigurable; and provides applications with a sequence of consistent views of the system membership. We demonstrate the utility of this membership service by using it in a novel distributed hash table called dBQS that provides atomic semantics even across changes in replica sets. dBQS is interesting in its own right because its storage algorithms extend existing Byzantine quorum protocols to handle changes in the replica set, and because it differs from previous DHTs by providing Byzantine fault tolerance and offering strong semantics. We implemented the membership service and dBQS. Our results show that the approach works well, in practice: the membership service is able to manage a large system and the cost to change the system membership is low.

63. Privacy-Preserving Updates to Anonymous and Confidential Databases.

Synopsis:

Suppose Alice owns a k-anonymous database and needs to determine whether her database, when inserted with a tuple owned by Bob, is still k-anonymous. Also, suppose that access to the database is strictly controlled, because for example data are used for certain experiments that need to be maintained confidential. Clearly, allowing Alice to directly read the contents of the tuple breaks the privacy of Bob (e.g., a patient's medical record); on the other hand, the confidentiality of the database managed by Alice is violated once Bob has access to the contents of the database. Thus, the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting Alice and Bob know the contents of the tuple and the database, respectively. In this paper, we propose two protocols solving this problem on suppression-based and generalization-based k-anonymous and confidential databases. The protocols rely on well-known cryptographic assumptions, and we provide theoretical analyses to proof their soundness and experimental results to illustrate their efficiency.

64. Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption.

Synopsis:

Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR=40 dB.

65. Replica Placement for Route Diversity in Tree-Based Routing Distributed Hash Tables.

Synopsis:

Distributed hash tables (DHTs) share storage and routing responsibility among all nodes in a peer-to-peer network. These networks have bounded path length unlike unstructured networks. Unfortunately, nodes can deny access to keys or misroute lookups. We address both of these problems through replica placement. We characterize tree-based routing DHTs and define MaxDisjoint, a replica placement that creates route diversity for these DHTs. We prove that this placement creates disjoint routes and find the replication degree necessary to produce a desired number of disjoint routes. Using simulations of Pastry (a tree-based routing DHT), we evaluate the impact of MaxDisjoint on routing robustness compared to other placements when nodes are compromised at random or in a contiguous run. Furthermore, we consider another route diversity mechanism that we call neighbor set routing and show that, when used with our replica placement, it can successfully route messages to a correct replica even with a quarter of the nodes in the system compromised at random. Finally, we demonstrate a family of replica query strategies that can trade off response time and system load. We present a hybrid query strategy that keeps response time low without producing too high a load.

66. Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs.

Synopsis:

The multihop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols,

including sinkhole attacks, wormhole attacks, and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the WSNs against adversaries misdirecting the multihop routing, we have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. Further, we have implemented a low-overhead TARF module in TinyOS; as demonstrated, this implementation can be incorporated into existing routing protocols with the least effort. Based on TARF, we also demonstrated a proof-of-concept mobile target detection application that functions well against an antidetection mechanism..

67. Robust Correlation of Encrypted Attack Traffic through Stepping Stones by Flow Watermarking.

Synopsis:

Network-based intruders seldom attack their victims directly from their own computer. Often, they stage their attacks through intermediate “stepping stones” in order to conceal their identity and origin. To identify the source of the attack behind the stepping stone(s), it is necessary to correlate the incoming and outgoing flows or connections of a stepping stone. To resist attempts at correlation, the attacker may encrypt or otherwise manipulate the connection traffic. Timing-based correlation approaches have been shown to be quite effective in correlating encrypted connections. However, timing-based correlation approaches are subject to timing perturbations that may be deliberately introduced by the attacker at stepping stones. In this paper, we propose a novel watermark-based-correlation scheme that is designed specifically to be robust against timing perturbations. Unlike most previous timing-based correlation approaches, our watermark-based approach is “active” in that it embeds a unique watermark into the encrypted flows by slightly adjusting the timing of selected packets. The unique watermark that is embedded in the encrypted flow gives us a number of advantages over passive timing-based correlation in resisting timing perturbations by the attacker. In contrast to the existing passive correlation approaches, our active watermark-based correlation does not make any limiting assumptions about the distribution or random process of the original interpacket timing of the packet flow. In theory, our watermark-based correlation can achieve arbitrarily close to 100 percent correlation true positive rate (TPR), and arbitrarily close to 0 percent false positive rate (FPR) at the same time for sufficiently long flows, despite arbitrarily large (but bounded) timing perturbations of any distribution by the attacker. Our paper is the first that identifies 1) accurate quantitative tradeoffs between the achievable correlation effectiveness - nd the defining characteristics

of the timing perturbation; and 2) a provable upper bound on the number of packets needed to achieve a desired correlation effectiveness, given the amount of timing perturbation. Experimental results show that our active watermark-based correlation performs better and requires fewer packets than existing, passive timing-based correlation methods in the presence of random timing perturbations.

68. Secure Service-Oriented Architecture for Mobile Transactions.

Synopsis:

The paper describes secure service-oriented architecture for mobiletransactions. The architecture comprises components, protocols, applicationsand interfaces and it provides various security services to various mobileapplications:Registration, Certification, Authentication, and Authorization of users,secure messaging at an application–level (end–to–end security), protectionof data in databases, and security services for protection of its owncomponents. The architecture is modular, integrated, extendible andscalable. The paper describes design of the architecture, the status of itscurrent implementation, and future research and development plans

69. The Geometric Efficient Matching Algorithm for Firewalls.

Synopsis:

Since firewalls need to filter all the traffic crossing the network perimeter, they should be able to sustain a very high throughput, or risk becoming a bottleneck. Firewall packet matching can be viewed as a point location problem: Each packet (point) has five fields (dimensions), which need to be checked against every firewall rule in order to find the first matching rule. Thus, algorithms from computational geometry can be applied. In this paper, we consider a classical algorithm that we adapted to the firewall domain. We call the resulting algorithm “Geometric Efficient Matching” (GEM). The GEM algorithm enjoys a logarithmic matching time performance. However, the algorithm's theoretical worst-case space complexity is O(n4) for a rule-base with n rules. Because of this perceived high space complexity, GEM-like algorithms were rejected as impractical by earlier works. Contrary to this conclusion, this paper shows that GEM is actually an excellent choice. Based on statistics from real firewall rule-bases, we created a Perimeter rules model that generates random, but nonuniform, rule-bases. We evaluated GEM via extensive simulation using the Perimeter rules model. Our simulations show that on such rule-bases, GEM uses near-linear space, and only needs approximately 13 MB of space for rule-bases of 5,000 rules. Moreover, with use of additional space improving heuristics, we have been able to reduce

the space requirement to 2-3 MB for 5,000 rules. But most importantly, we integrated GEM into the code of the Linux iptables open-source firewall, and tested it on real traffic loads. Our GEM-iptables implementation managed to filter over 30,000 packets-per-second on a standard PC, even with 10,000 rules. Therefore, we believe that GEM is an efficient and practical algorithm for firewall packet matching.

70. Fast Matrix Embedding by Matrix Extending.

Synopsis:

When designing steganographic schemes, matrix embedding is an efficient method for increasing the embedding efficiency that is de- fined as an average number of bits embedded via per change on the cover. Random linear code-based matrix embedding can achieve high embedding efficiency but cost much in computation. In this paper, we propose a method to increase the embedding speed of matrix embedding by extending the matrix via some referential columns. Compared with the original matrix embedding, the proposed method can exponentially reduce the computational complexity for equal increment of embedding efficiency. Experimental results also show that this novel method achieves higher embedding efficiency and faster embedding speed than previous fast matrix embedding methods, and thus is more suitable for real-time steganogaphic systems.

71. Joint Relay and Jammer Selection for Secure Two-Way Relay Networks.

Synopsis:

In this paper, we investigate joint relay and jammer selection in two-way cooperative networks, consisting of two sources, a number of intermediate nodes, and one eavesdropper, with the constraints of physical-layer security. Specifically, the proposed algorithms select two or three intermediate nodes to enhance security against the malicious eavesdropper. The first selected node operates in the conventional relay mode and assists the sources to deliver their data to the corresponding destinations using an amplify-and-forward protocol. The second and third nodes are used in different communication phases as jammers in order to create intentional interference upon the malicious eavesdropper. First, we find that in a topology where the intermediate nodes are randomly and sparsely distributed, the proposed schemes with cooperative jamming outperform the conventional nonjamming schemes within a certain transmitted power regime. We also find that, in the scenario where the intermediate nodes gather as a close cluster, the jamming schemes may be less effective than their nonjamming counterparts. Therefore, we introduce a hybrid scheme to switch between jamming and nonjamming modes. Simulation results validate our theoretical analysis and show that the hybrid switching scheme further improves the secrecy rate.

72. Color Extended Visual Cryptography Using Error Diffusion.

Synopsis:

Color visual cryptography (VC) encrypts a color secret message into color halftone image shares. Previous methods in the literature show good results for black and white or gray scale VC schemes, however, they are not sufficient to be applied directly to color shares due to different color structures. Some methods for color visual cryptography are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to suspicion of encryption. This paper introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. Comparisons with previous approaches show the superior performance of the new method.

73. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing.

Synopsis:

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in

dealing with access control for outsourced data in cloud computing with comprehensive experiments.

74. OAuth Web Authorization Protocol

Synopsis:

Allowing one Web service to act on our behalf with another has become increasingly important as social Internet services such as blogs, photo sharing, and social networks have become widely popular. OAuth, a new protocol for establishing identity management standards across services, provides an alternative to sharing our usernames and passwords, and exposing ourselves to attacks on our online data and identities.

75. On Privacy of Encrypted Speech Communications.

Synopsis:

Silence suppression, an essential feature of speech communications over the Internet, saves bandwidth by disabling voice packet transmissions when silence is detected. However, silence suppression enables an adversary to recover talk patterns from packet timing. In this paper, we investigate privacy leakage through the silence suppression feature. More specifically, we propose a new class of traffic analysis attacks to encrypted speech communications with the goal of detecting speakers of encrypted speech communications. These attacks are based on packet timing information only and the attacks can detect speakers of speech communications made with different codecs. We evaluate the proposed attacks with extensive experiments over different type of networks including commercial anonymity networks and campus networks. The experiments show that the proposed traffic analysis attacks can detect speakers of encrypted speech communications with high accuracy based on traces of 15 minutes long on average.

76. Packet-Hiding Methods for Preventing Selective Jamming Attacks.

Synopsis:

The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launchpad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this

work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.

77. Recommendation Models for Open Authorization.

Synopsis:

Major online platforms such as Facebook, Google, and Twitter allow third-party applications such as games, and productivity applications access to user online private data. Such accesses must be authorized by users at installation time. The Open Authorization protocol (OAuth) was introduced as a secure and efficient method for authorizing third-party applications without releasing a user's access credentials. However, OAuth implementations don't provide the necessary fine-grained access control, nor any recommendations, i.e., which access control decisions are most appropriate. We propose an extension to the OAuth 2.0 authorization that enables the provisioning of fine-grained authorization recommendations to users when granting permissions to third-party applications. We propose a multicriteria recommendation model that utilizes application-based, user-based, and category-based collaborative filtering mechanisms. Our collaborative filtering mechanisms are based on previous user decisions, and application permission requests to enhance the privacy of the overall site's user population. We implemented our proposed OAuth extension as a browser extension that allows users to easily configure their privacy settings at application installation time, provides recommendations on requested privacy permissions, and collects data regarding user decisions. Our experiments on the collected data indicate that the proposed framework efficiently enhanced the user awareness and privacy related to third-party application authorizations.

78. Steganography Bit Plane Complexity Segmentation (BPCS) Technique.

Synopsis:

Steganography is an ancient technique of data hiding. Steganography is a technique in which secret data is hidden into vessel image without any suspicion. All other traditional

techniques have limited data hiding capacity and can hide up to 15% of data amount of vessel image. This paper focuses on basic steganography and various characteristics necessary for data hiding. More importantly, the paperimplements a steganographic technique that has hiding capacity up to 50 – 60% [8] [9]. This technique is called Bit Plane Complexity Segmentation (BPCS) Steganography. The main principle of BPCS technique is that, the binary image is divided into informative region and noise-like region. The secret data is hidden into noise-like region of the vessel image without any deterioration. In our experiment, we used the BPCS Principle by “Eiji Kawaguchi & Richard O. Eason” and experimented by using two images i) vessel imageof 512 x 512 size ii) secret image of 256 x 256 size. We performed this experiment for 3 different sets of images and calculated image hiding capacity.