doi:10.1093/comjnl/bxr101

Capsule Reviews

FAIROUZ KAMAREDDINE

The Capsule Reviews are intended to provide a short succinct review of each paper in the issue in order to bring it to a wider readership. The Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of *The Computer Journal* and is based in the Department of Mathematical and Computer Sciences at Heriot-Watt University, Edinburgh, UK.

Surveying Port Scans and Their Detection Methodologies. MONOWAR H. BHUYAN, D.K. BHATTACHARYYA AND J.K. KALITA
Network defenders can identify malicious scans using scan statistics on a real-life network. A port scan is a collection of hostile Internet searches for open ports, through which intruders gain access to computers. As stated in the paper, it is useful for system administrators and other network defenders to detect port scans as a technique for recognizing precursors to serious attacks. As a starting point for people trying to understand, evaluate, deploy or create port scan detection techniques, the authors gives a survey of port scans and their detection methodologies. Their intention is to enumerate and compare the published single-source as well as distributed techniques used for port scan detection and to explain their abilities as well as their limitations. Port scanning techniques are introduced into two broad categories: single-source port scans and distributed port scans, and various port scan detection approaches available in the literature are classified into two different categories: single-source approaches and distributed approaches, and are explained from different perspectives (algorithmic, visual, clustering-based, rule-based, threshold-based, etc.). Finally, the authors discuss commonly used evaluation data sets and criteria for evaluating scan detectors and outline challenges and future directions.

Refinements of Miller's Algorithm over Weierstrass Curves Revisited. DUC-PHONG LE AND CHAO-LIANG LIU
The paper starts by the observation that the efficient algorithms for Weil/Tate pairing computation play a very important role in pairing-based cryptography and that the best known method for computing Weil/Tate pairings is based on Miller's algorithm for rational functions from scalar multiplication of divisors. Due to its importance, many improvements have been carried out on the Miller algorithm. This paper extends the so-called Blake–Murty–Xu method, shows how to eliminate all of the vertical lines in Miller's algorithm and compares the proposed algorithm and a modified version with the existing algorithms. After an introduction to the backgrounds, the definitions of the Weil/Tate pairings, Miller's algorithm for Weil/Tate pairing computation and the Blake–Murty–Xu method for reducing vertical lines in Miller's algorithm, the authors give their own improvements on Miller's algorithm. This is followed by a performance analysis of the proposed algorithm and a comparison with the original Miller algorithm, the Blake–Murty–Xu refinements, the algorithm of Barreto *et al.* for computing the Tate pairing on curves with even embedding degrees, and the algorithm of Lin *et al.* for computing the pairings on curves with the embedding degree $k = 9$. A further modification of the proposed algorithm is given and experiments are reported.

A Truly Random Number Generator Based on a Pulse Excited Cross Coupled Chaotic Oscillator. SALIH ERGUN
Chaotic oscillators are one of the techniques used for random number generation; however, they do not realize well high-performance integrated circuit (IC) design issues. The author has previously established that continuous-time chaotic oscillators can be used to realize random number generators (RNGs), and in this paper, he explains the derivation mechanism of the chaotic oscillator that is suitable for high-performance IC realization. Moreover, he introduces the design of a Truly RNG (TRNG), which relies on generating non-invertible random binary bits according to regional distributions from one of the waveforms of the chaotic oscillator. Numerical and experimental results are given to illustrate the feasibility of the proposed design and its usage as a high-performance IC TRNG.

Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks. RUBEN RIOS AND JAVIER LOPEZ
The authors take the view that in wireless Sensor Networks (WSNs), sensor nodes represent the senses, the communication channels can be regarded as the nerves and the base station depicts the brain. Sensors can include temperature, humidity, pressure, acoustic and radiation sensors. However, there are also network privacy considerations that might leak information about the network itself. Most of the work dealing with source-location privacy in WSNs have focused on randomly sending

every packet on a different route in order to minimize the chances of an attacker finding the source of the messages. This method may not be fully secure and hence, this paper focuses on the Context-Aware Location Privacy (CALP) approach, which takes advantage of sensor nodes' context-awareness in order to detect the presence of a mobile adversary in their surroundings so that packets are routed in a more efficient and privacy-preserving manner. After an overview of the related work, the authors present the main assumptions, the network model under consideration and the features that define the type of attacker. Then, the CALP scheme is presented and takes advantage of the ability of sensor nodes to perceive the existence of moving objects in their vicinity and allows sensor nodes to modify their routing tables in order to circumvent the region under the control of the adversary. The CALP protection mechanism is applied to a shortest path routing algorithm that makes greedy forwarding decisions by selecting locally optimal (minimally deviating from the straight line connecting the node and the destination) neighbours. Two versions of the shortest-path CALP routing are devised. Extensive simulations are conducted to evaluate the performance and privacy protection level of the proposed shortest-path CALP routing mechanism, and the impact of the security perimeter size on the privacy protection level as well as the mean path length.

Compositional Approach to Quantify the Vulnerability of Computer Systems. HOSSEIN HOMAEI AND HAMID REZA SHAHRIARI

Any vulnerability measurement approach needs to consider many factors, including the skill of the attacker, the attack duration, the size of the system, etc. This paper proposes a compositional model to quantify the vulnerability of computer systems where the vulnerability quantity of systems is calculated using the vulnerability measures of constitutive components. After a survey of related work, the modelling process of computer systems (which consists of a set of states connected to each other by some transitions) is provided along with an attacker model to evaluate the security of a computer system and the composition of attacker and system models. Thereafter, a metric to quantify vulnerability is proposed, where the less it costs to reach an unauthorized state, the more vulnerable is the state. The vulnerability of the whole system is evaluated in terms of the vulnerability of each state. Since the state space of complex systems is very large and complicated, a compositional method to measure the vulnerability of complex systems is applied. This method is based on compatible unauthorized states, compatible systems and operators to combine components and construct composite systems. The proposed compositional method satisfies four theorems to measure the vulnerability of complex systems. Each such theorem studies one of the compositional operators. A case study is given to illustrate the compositional vulnerability measurement process in a sample. This is followed by a discussion, a conclusion and some proposed future work.

Correlation Keystroke Verification Scheme for User Access Control in Cloud Computing Environment. KAI XI, YAN TANG AND JIANKUN HU

As the core security component, user access control (UAC) plays a vital role in recent cloud computing systems. The most widely deployed user authentication mechanism is based upon passwords. However, passwords are vulnerable to attacks and furthermore, knowledge-based authentication mechanisms can only ensure that the person possesses the right information, and cannot confirm that the person is a legal user. This paper focuses on authentication in terms of user verification and argues that physiological biometrics may not be the best choice for cloud computing systems and that authentication via keystroke dynamics may avoid some of the concerns related to physiological biometrics. The paper addresses both authentication accuracy and scalability/computational efficiency. After an introduction to the related work, including the Degree of Disorder (DoD), keystroke authentication method that compares two different sets of sorted trigraphs and measures the difference in the ordering between them, the Gunetti and Picardi (GP) identification-like authentication method and the correlation pattern recognition (CPR) biometric traits recognition method, the authors propose a way to transform n-graph DoD to an equivalent correlation-oriented feature called n-graph disorder vector (nGdv). This allows the authors to develop two CPR-based keystroke verification methods (nGdv-V and nGdv-C) using nGdv. The performance of the system is evaluated by measuring the number of correct authentication, false authentication and computational efficiency. It is concluded that the nGdv-C significantly improves False Rejection Rate (FRR) and authentication times and that high accuracy and fast speed make nGdv-C as one of the most promising keystroke solution for UAC in the clouding computing environment.

Cryptanalysis of an Off-Line Electronic Cash Scheme Based on Proxy Blind Signature. YONG YU, YI MU, GUILIN WANG AND YING SUN

In a proxy signature scheme, an original signer can delegate its signing power to a proxy signer. Blind signature is a protocol for obtaining a digital signature from a signer, while the signer can neither learn the signed message nor recognize the signature. A proxy blind signature scheme captures the features of both proxy signature and blind signature and can be applied to the construction of an e-cash scheme. Several proxy blind signature schemes have been proposed in the literature, including a provably secure proxy blind signature from bilinear pairing, which was also used as a base for an off-line e-cash scheme. It was claimed in the literature that both the proposed proxy blind signature and the off-line e-cash schemes are secure and satisfy all the desirable security requirements. This paper shows that the proxy blind signature scheme in question is insecure, since it is vulnerable to an original signer's forgery attack and that the off-line e-cash scheme has some security flaws.

On the Hardness of the Sum of *k* Mins Problem. HASSAN JAMEEL ASGHAR, JOSEF PIEPRZYK AND HUAXIONG WANG
Currently, the prevalent form of identification to a remote server for humans is password-based authentication. In order to avoid eavesdropping, there are efforts to construct secure protocols that can authenticate users with an insecure computer terminal. Hard mathematical problems have been used to construct protocols that are both usable and secure. One such protocol (HB) is NP-hard and is based on the problem of learning parity in the presence of noise. Another such protocol is based on the sum of k mins problem. This paper shows that a version of the sum of k mins problem is NP-Complete and W-Hard. After a brief discussion of related work, the authors introduce the sum of k mins problem, its matrix representation, the sum of k Mins protocol and a generalization of the sum of k mins problem. Formal reduction of one problem to another is used to show the main result of NP-Completeness and W-Hardness of the so-called modular sum of k Mins.

Secure Image Retrieval Based on Visual Content and Watermarking Protocol. JUN ZHANG, YANG XIANG, WANLEI ZHOU, LEI YE AND YI MU
Content-based image retrieval (CBIR) aims to search digital images from large image data sets based on their visual content described by features such as color, texture and shape. The authors argue that improving the retrieval performance in CBIR has attracted a lot of attention, while very few efforts address security concerns. The paper focuses on security issues such as user rights and privacy and shows that conventional CBIR systems suffer from the user right problem and that the user's privacy can be protected by conventional copy deterrence schemes based on digital watermarking. After an introduction to the related work and to the buyer–seller watermarking protocol, which will be used in the proposed image retrieval protocol, the authors outline their design goals and the problems that a two-party image-retrieval watermarking protocol should solve. Then, the proposed two-party image-retrieval watermarking protocol is presented by first introducing the various crypto primitives (such as encryption and homomorphic encryption, signature and perceptual hash) needed for the protocol and then by giving its two sub-protocols: the protection protocol and the arbitration protocol. In the protection protocol, the interaction occurs between the user and the service provider of CBIR. The arbitration protocol is designed to trace the pirate responsible and gather undeniable evidence, when an unauthorized copy Y of the user's query image X is found. Thereafter, the authors carry out security analysis in order to show how the proposed image-retrieval watermarking protocol can achieve the assumed design goals. A discussion follows on the quality of watermarked digital content, the disadvantages of using the proposed protocol and denial of service (DoS) attacks. Finally, the authors report on empirical research on CBIR with the proposed security mechanism and carry out a number of retrieval experiments to demonstrate the practicality and effectiveness of the proposed scheme

Enforcing Role-Based Access Control for Secure Data Storage in the Cloud. LAN ZHOU, VIJAY VARADHARAJAN AND MICHAEL HITCHENS
The authors argue that the greater the sensitivity of the data stored in the cloud, the more stringent the security requirements on its access need to be. One approach to safeguarding data is to use cryptographic techniques to encrypt the data before storing it in the cloud. In this case, the problem of achieving secure access to data stored in the cloud is transformed into the problem of access to keys and this requires an access control and a key distribution policy. Since the cloud provider may not be trusted due to the distributed nature of the cloud architecture, users cannot rely on the service provider in the cloud environment to enforce the access control. The authors propose a hybrid scheme called role-based encryption (RBE), that combines access control with cryptography and key distribution to address security requirements for data storage in the cloud. After an introduction to the related work, the concepts of broadcast encryption (BE) and ID-based BE are surveyed before formulating the proposed RBE framework and listing its security properties. The hybrid RBE scheme is based on ID-based BE and is illustrated by two small examples. Next, the proposed hybrid RBE scheme is analysed and it is shown that it is selective-ID secure(IND-sID) and revocable-ID secure(sRID). Moreover, the efficiency of the scheme is studied and it is shown that it has constant-size ciphertext and decryption key and that the role memberships of the users are no longer decided by a single trusted party. Instead, they are controlled by role managers, who could be different for each role. It is furthermore shown that the proposed scheme, with its constant size ciphertext and decryption key, is more efficient for large-scale systems, and the decryption only requires one computation round. A discussion on how the proposed scheme can be improved is given. In particular, the authors discuss the implementation and how to optimize the decryption strategy.

Fully Deniable Message Authentication Protocols Preserving Confidentiality. LEIN HARN, CHIA-YIN LEE, CHANGLU LIN AND CHIN-CHEN CHANG
The authors argue that most secure communications consider the two basic security properties of message confidentiality and message authentication and that before exchanging communication messages, a key establishment protocol (which must provide confidentiality and authentication for session keys) is used to construct the session keys for the communication participants. Although the objective of message authentication can be achieved by using the digital signature, there is still a potential threat to the sender of the message and deniable authentication was proposed to overcome this threat. There are two types of deniability: plausible deniability

and full deniability; however, most existing deniable protocols only provide 1-out-of-2 deniability. This paper addresses this issue and propose two communication protocols with message confidentiality and authentication that can achieve full deniability (referred to in the article as 1-out-of-∞ deniability). The correctness of the proposed protocols is analysed.

The Microcosmic Model of Worm Propagation. YINI WANG, SHENG WEN, SILVIO CESARE, WANLEI ZHOU AND YANG XIANG
The authors argue that worms and their variants are widely believed to be one of the most serious challenges to address in network security research, and that Security experts routinely uncover software vulnerabilities and then issue software patches and upgrades. This, according to the authors, lead to the need to quantify an appropriate time for patching vulnerabilities and to characterize worm propagation. The paper lists a number of issues that are important to guarantee in any model of worm propagation such as propagation probability/time delay, etc., and states that a microcosmic model can be beneficial for describing the propagation procedure. The authors create a microcosmic landscape on worm propagation and generate a set of optimized patch strategies to minimize the number of infected peers. After a discussion of the related work, including the macroscopic and microscomic worm propagation models, the authors set out to present their propagation model that is used to simulate the propagation process of worms and to estimate an optimized patch strategy. An important feature of their model is the propagation matrix (PM) that models worm propagation, and simulates the microcosmic spreading procedure of worms. In particular, the procedure of worms spreading is studied in detail through three factors (infectious state, vulnerability distribution and patch strategy) and the authors provide effective patching strategies. Extensive experiments in different scenarios are carried out by a series of simulations that focus on these various factors and their effects. Results illustrate the benefits of the proposed method and there is a discussion of the limitations and of the open issues that remain.

CORPS: Building a Community of Reputable PeerS in Distributed Hash Tables. ERIKA ROSAS, OLIVIER MARIN AND XAVIER BONNAIRE
The authors argue that in a Peer-to-Peer (P2P) network, the lack of central control, the considerable number of peers and the high dynamism of the network make it very hard to build trust among peers. This is especially the case since a P2P network includes untrusted nodes from an open environment, such as the Internet. The goal of this paper is to propose an efficient and simple way to build a group of trusted nodes (called Trusted Ring) within Distributed Hash Tables (DHT) that is based on a reputation system. First, an introduction to the backgrounds is given, which includes a description of the type of P2P overlay and an overview of Reputation Systems that are used to identify trustworthy peers. Then, the problem is formalized for a DHT network in which each node has an associated reputation, and the assumptions and desired properties of the system are listed. Thereafter, the membership algorithm (CORPS) used to build the Trusted Ring is described. The Trusted Ring provides an efficient way to contact a trustworthy node in order to involve it in a pseudo-trusted service. An example of how to use the Trusted Ring for a trusted routing service is given, followed by the theoretical evaluation of the Trusted Ring and the benefits in the case of trusted routing. Portability and security issues of the proposed solution are discussed and followed by comparison and related work.