doi:10.1093/comjnl/bxs034

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.

Secure-TWS: Authenticating Node to Multi-user Communication in Shared Sensor Networks. LEONARDO B. OLIVEIRA, AMAN KANSAL, CONRADO P.L. GOUVEA, DIEGO F. ARANHA, JULIO LOPEZ, BODHI PRIYANTHA, MICHEL GORACZKO AND FENG ZHAO

While the sharing of sensors over the Internet is not new, recent works have demonstrated the usefulness of methods that connect low-power sensor nodes directly to applications, locally and over the Internet, without intermediary gateways. This paper describes the implementation of a security solution for sensor nodes that are shared by multiple users. This implementation complements the network layer and application layer protocols available for these scenarios with support for security. It achieves authentication and provides experimental evaluations that help decide among key design choices involved. The developed security solution is called Secure Tiny Web Service (Secure-TWS). The authors identify first the key security primitives that are applicable for providing authentication and select a small number of appropriate design options that need to be evaluated for enabling efficient implementations. The design space is discussed and the overall authentication procedure for the security scenario of interest is setup. The design parameters and resource overheads that affect the choice of digital signature schemes for shared sensor node usage are discussed together with the implementation issues faced during the implementation of Secure-TWS. The performance and resource overheads of the Secure-TWS solution are evaluated and compared with the literature. In particular, the evaluation concentrates on storage, computation and communication overheads.

Dynamic State-Based Security Architecture for Detecting Security Attacks in Virtual Machines. UDAYA KIRAN TUPAKULA AND VIJAY VARADHARAJAN

Internet attackers are becoming more competent at exploiting vulnerabilities in software and at generating new types of attacks. Furthermore, the dynamic nature of attacks makes them difficult to detect and prevent. The authors state that there is a considerable research interest in the development of Virtual Machine Monitors (VMM)-based security tools such as intrusion detection systems (IDSs) and propose a security architecture based on VMM to deal efficiently with security attacks in the Internet. After a review of work relevant to the proposed architecture, the authors set out the requirements and design choices for a comprehensive IDS architecture using VMMs. These requirements include the need to: adopt a proactive approach, keep track of the dynamic changes, identify attacks with minimal false positives and false negatives and at a fine granular level, and support variable security levels with different overheads for different applications. Then, an overview of the proposed virtual machine-based architecture is given and followed by its operations (at source/destination and the sharing of information to detect attacks) and its components used to deal with different types of attacks on virtual machines (which are assumed to be trusted and secure). The architecture is named VICTOR (Virtual machine Intrusion deteCTOR). An implementation of the VICTOR architecture was used to conduct performance analysis with varying number of virtual machines. A detailed analysis of one malware using the proposed architecture is presented in the paper and followed by a discussion on the optimization of VICTOR.

Attacking Anonymous Web Browsing at Local Area Networks Through Browsing Dynamics. SHUI YU, WANLEI ZHOU, WEIJIA JIA AND JIANKUN HU

Traffic analysis is a powerful attack tool against anonymity, and most systems focus on safeguarding against traffic analysis attacks. The authors state that the vulnerability of the end-user aspect (the connection between the end user and the anonymous network) has yet to be explored and focus on revealing a brand new attack strategy on anonymous web browsing systems, which employs end-user browsing dynamics to break the user's anonymity. A specific hidden Markov model (HMM) is established for the proposed attack method. After an introduction to the related work and to the dynamics of the web, the problem settings are given and used to demonstrate the new attack. The HMM model for browsing dynamics based attack is given together with a method for estimating the parameters of the model and for inferring the browsed pages. The algorithm to execute the browsing dynamics based attack is given and it is shown how to break the anonymity of the user's web browsing. In order to evaluate the effectiveness of the proposed attack method, the authors collected web browsing dynamics data for 1 week at a Chinese backbone network center.

Satisfying Privacy Requirements Before Data Anonymization. XIAOXUN SUN, HUA WANG, JIUYONG LI AND YANCHUN ZHANG

Privacy risks of publishing microdata are well known and although privacy preservation on relational data has been extensively studied, it remains a challenge to protect individuals' privacy in large survey rating data. According to the authors, there is no current research addressing the issue of how to efficiently determine whether the survey rating data 'satisfy' the privacy requirement. It is stated that the lack of a clear set of personal identifiable attributes together with its high dimensionality and sparseness make the determination of the satisfaction problem challenging. This paper considers the privacy risk in publishing anonymous survey rating data and aims to solve the Satisfaction Problem. In order to do so, the authors utilize the largeness and sparseness properties to develop a novel slicing technique. After a discussion of the motivation and related work, the anonymity model is defined and its properties are characterized. Thereafter, the satisfaction problem is formalized and a slicing technique is developed based on the properties of the anonymity model. It is shown how this technique is used to determine the Satisfaction Problem and the complexity of the slicing algorithm is analyzed. Finally, the time/space efficiency of the proposed slicing algorithm is experimentally evaluated and future works are discussed.

Improved Anonymous Multi-receiver Identity-Based Encryption. HUNG-YU CHIEN

This paper focuses on multi-receiver identity-based encryption schemes that take into consideration the receiver's privacy. The author reviews earlier schemes for protecting privacy and anonymity and concentrates on a recent scheme proposed by Fan, Huang and Ho. The author shows that this scheme of Fan *et al.* fails in protecting the receiver's anonymity. To overcome this weakness in the Fan *et al.* scheme, the author proposes a new scheme aimed at enhancing security and computational performance. The author shows that the security and the receiver anonymity of his proposed scheme is secure if the Co-Bilinear Diffie-Hellman (Co-BDH) problem is hard. The performance of the proposed scheme is compared with that of the Fan et al. scheme in terms of computation and communication.

On F5 Steganography in Images. XIANGYANG LUO, FENLIN LIU, CHUNFANG YANG, SHIGUO LIAN AND DAOSHUN WANG

Steganography is a potential technique to transmit a secret message through a digital file and is considered broken when the presence of a secret message can be established even though to extract the secret message, one needs quantitative steganalysis where the length of the message, the embedding/modification ratio, etc., can be estimated. F5 is a steganographic method that hides data into JPEG images and introduces a matrix encoding technique to improve the embedding efficiency. Although existing steganalysis methods can estimate the modification ratio of F5 and its improved version nsF5, there still exist a large number of estimation errors. This paper proposes two steganalysis methods to estimate the modification ratio of F5 and nsF5 based on relative entropy used to measure the distance between the coefficient histogram of the given image and the estimated one. First, the authors introduce F5 and nsF5 and then propose their methods for estimating modification ratio based on relative entropy for both F5 and nsF5. Thereafter, the performance of the proposed methods is compared with those of the so-called Least Square Method Support Vector Regression method.

Certificateless Signatures: New Schemes and Security Models. XINYI HUANG, YI MU, WILLY SUSILO, DUNCAN S. WONG AND WEI WU

Certificateless cryptography does not require any certificates to ensure the authenticity of public keys. Instead, it relies on the existence of a semi-trusted third party Key Generation Center (KGC), who has the master secret key. The KGC might engage in adversarial activities which fall under the so-called Type I Adversary and Type II Adversary. There is a debate on how to define these two types of adversaries in the literature. After a review of certificateless encryption (CLS) and of the basic types of adversaries in CLS, the authors state that it is worthwhile to define the adversary against (CLS) in the real world and define different sign oracles that can be accessed by different adversaries and divide them according to their attack power. Three kinds of attackers are introduced to the CLS: Normal Adversary, Strong Adversary and Super Adversary. Combined with Type I Adversary and Type II Adversary, this leads to Normal Type I Adversary, Strong Type I Adversary, etc., against which the authors formulate security models of CLS. In particular, the authors discuss security against: a normal type I adversary, a strong type I adversary, a super type I adversary, and type II adversaries. This results in two CLS schemes that are proved to be secure as follows: the first is secure against a Normal Type I adversary and Super Type II adversary, the second is secure against a Super Type I and Type II adversary. The proposed schemes are compared with other CLS schemes in the literature. Since the proposed schemes are built from pairings on elliptic curves that can be computationally expensive, the authors give two server-aided verification protocols (one for each scheme) to help reduce the computational cost.

Efficient Revocable ID-Based Encryption with a Public Channel. Yuh-Min Tseng and Tung-Tso Tsai

Since a user's identity (ID) in the ID-based public key system (IDPKS) represents his/her public key, it is not desired to be changed. In IDPKS however, we face the critical problem of how to revoke misbehaving/compromised users. For these users, any ID-based or certificate-based public key settings must provide a revocation solution. Furthermore, for ID-based encryption (IBE), only the system's public parameters and the user's ID are involved in the encryption procedure, and hence it is difficult to notify senders that a particular ID was revoked. The authors address these revocation problems in the IDPKS and present new revocable IBE (RIBE). After a review of the related work and the needed preliminaries such as bilinear pairings defined on elliptic curves over finite fields and the security assumptions used in the paper, the new mechanism RIBE is introduced. First, the formal framework of a RIBE is defined with a public channel and its semantic security discussed. Then, five algorithms are described to build the concrete basic RIBE scheme. These include the system setup, the initial key extract, the time key update, the encryption and the decryption procedures. After a study of the security analysis of the basic RIBE, transformation techniques are applied on the basic RIBE to obtain a full RIBE scheme which again consists of five algorithms as above. Finally, performance, computational costs and transmission size are analyzed.

Predicting the Propagation Path of Random Worm by Subnet Infection Situation Using Fuzzy Reasoning. Lina Zhu, Li Feng and Zuochang Zhang

According to the authors, researching a worm's propagation characteristics and predicting its behavior are essential for proactive intrusion detection/prevention systems. Since the propagation of a worm and its offspring will form a path, the aim of this paper is to predict the worm's track by estimating the infection situation of the subnet. The authors propose two significant indices: the subnet infection time and subnet infection frequency, and use fuzzy theory to deduce the infection situation for each subnet. After a review of the related work and the motivations behind the paper, the authors detail the infection measurement for a subnet through the specification of the two indices and estimate the infection situation using fuzzy reasoning. To validate the model for predicting the network worms' propagation direction, a simulated large-scale network is designed and two experiments are carried out: one using the User Datagram Protocol and the other using the Transmission Control Protocol, and the worm propagation path is illustrated.