Foreword and Editorial

International Journal of Security and Its Applications

We are very happy to publish this issue of an International Journal of Security and Its Applications by Science and Engineering Research Support soCiety.

This issue contains 32 articles. Achieving such a high quality of papers would have been impossible without the huge work that was undertaken by the Editorial Board members and External Reviewers. We take this opportunity to thank them for their great support and cooperation.

The paper “A Key Distribution Scheme for WSN Based on Deployment Knowledge and Dual-Key Pools” propose a novel key distribution for WSN in a cell model based on the deployment and the dual-key pools. Each cell has a key pool consisted of two types of key pool: type Sa and type Sb. Both the key establishment probability and the security are improved by the extended key pool of type Sa, the sharing random numbers and the hash function. Compared with Du scheme and q-composite scheme, the simulation results show that the KDPK scheme performs the best in the pair-wise key establishment probability, the invulnerability and the node storage space.

Paper “Issues toward Networks Architecture Security for LTE and LTE-A Networks” illustrated the security architectures by the 3GPP standard. It further discussed the drawbacks existing in the security architecture of the LTE wireless networks. In this paper, several security issues of the LTE and LTE-A networks have been discussed. First, it illustrates an overview of the LTE Network Architecture. Second, LTE security architecture is shown as well. Third, some drawbacks in LTE security framework are discussed in Section 4. Finally, some open issues will be talked, and hopefully this will be a guideline for the new learners.

In the paper “Protecting Seaport Communication System by Steganography Based Procedures”, introduces a technique of Steganography, that is to say - transmitting encrypted messages in images compressed by the well-known JPEG format. In point of fact, the system modifies the pictures a bit, but this modification is totally unnoticeable. The image seems to be an immaculate picture, while truly the picture does include some extra information.

The paper “Research on Distinguish the Accounting Information Distortion Based on the Principle Components-logistic Regression Model” combines the method of principal component analysis with logistic regression method. Then it selects variables from the financial data that reflect the profitability, turnover, the establishment of the enterprise and some other perspectives. This accounting information distortion detection model is created by improving the method and index selection which has a higher correct recognition rate.

The Authors of “A Study of Key management Protocol for Secure Communication in Personal Cloud Environment” suggested key management generates and contents communication method to enhance security and supplement vulnerability about personal information management on personal cloud circumstance. It enables the service for user
through generating each user authority key after transferring ID and PW to Key Server by client.

Paper “Attacks and Threats on the U-Healthcare Application with Mobile Agent” analyzed the characteristics of U-healthcare systems. The use of a mobile agent in healthcare system under wireless network environment gives an opportunity to offer better services for patients and staffs such as doctors and nurses because of its mobility. But, optimized security protocols and schemes between sensor and patient device are essential for high performance and security problem in U-healthcare system. But a lot of threats, attacks and vulnerability are induced because of limited resources such as small memory and low computation capability in wireless sensor network.

In the paper “A Composite Intelligent Method for Spam Filtering” analyses several common algorithms for spam filtering and shows the advantages and disadvantages of these algorithms for spam filtering. Each algorithm is only suitable for filtering specific spam. Some algorithms are suitable for Chinese, and some algorithms perform well in English. In a lot of spam, it is not reliable and inefficiency to using a single algorithm to separate out spam. Thereby, in order to improve the accuracy and efficiency of spam filtering, composite intelligent algorithm, which integrates and improves the existing algorithms by utilizing the advantages of previous algorithms and avoiding their shortages, is proposed.

The paper “Quantum Chaotic Image Encryption with One Time Running Key” proposed a new image encryption scheme based on quantum chaos to improve image encryption mechanism and enhance the security of pixel value transformation. In the phase of key generation, running key related to plaintext is generated by cipher-text successively disturbing chaotic component. In the process of encryption, polynomial multiplication in Galois field is first introduced to perform pixel encryption and then the cipher-text is encrypted again with cipher-text feedback mechanism. The experiment results show that the introduction of disturbing mechanism implements one time running-key stream, minimization of dynamical degradation of digital chaos, and resistance to reconstruction attack.

The paper “A Block Encryption Scheme for Secure Still Visual Data based on One-Way Coupled Map Lattice” proposes a new scheme for secure still visual data with a block cipher structure, which is composed of three parts: encryption, decryption and key generator. The encryption process based on cryptographic primitive operations and Boolean functions is proposed. A key generator based on one-way coupled map lattice (OCML) is derived.

The Authors of “Approaches for Testing and Evaluation of XACML Policies” describes a test automation framework dedicated to test XACML based security policies. This can be implemented as a standalone testing framework or part of a web, enterprise, or cloud infrastructure. Test automation can improve quality without the need for extensive resources. It proposed a test automation framework to generate, execute and evaluate test cases on XACML policies.

Paper “A Sticker-Based Model Using DNA Computing for Generating Real Random Numbers” designs the DNA-based RNG in sticker mode in such a way that always generate equal numbers of 0s and 1s and consequently passing frequency test with 100% of success. Besides the frequency test, generated random values were subjected to run and serial tests.
(proposed by NIST for randomness evaluation) where the achieved result prove the high quality of generated random values.

The paper “End-to-End Authentication Protocols for Personal/Portable Devices over Cognitive Radio Networks” reviews the first industrial standards for personal/portable devices in the TVWS from ECMA-International focused on the security aspects. After that, it point out the lack of security facilities in the standard, which does support the link-to-link security but not for the end-to-end security, and then propose two location-based authentication protocols to cope up with the deficiencies over cognitive radio networks.

Paper “Advanced Mobile Security System Operated by Bioelectrical Sensor” proposed an advanced security system that can increase password strength without modifying password length or increasing alphabet character variation. It presents an implementation of an intuitive password system that combines muscle activation to enhance password complexity.

In the paper “Cryptanalysis and Improvement of a Password-Based Authenticated Three-Party Key Exchange Protocol”, identified that the three-party PAKE protocol due to Kim and Choi is not secure against an offline dictionary attack in the presence of a malicious insider. The attack highlights again the difficulty of designing a secure yet efficient PAKE protocol in the password-only three-party protocol. This work also demonstrated that the existence of the dictionary attack implies insecurity of Kim and Choi’s protocol in the in distinguish ability-based security model of Bellare, Pointcheval and Rogaway.

The paper “Cryptanalysis of a Multi-use CCA-secure Proxy Re-encryption Scheme” propose an improvement for Wang-Multi-Use-PRE to resist Zhang’s attack. But it also found that different with single-hop PRE, multi-use PRE without randomize encrypt key in its re-encryption algorithm could be vulnerable to attack. According to this principle it finds a new type attack to multi-use CCA-secure PRE named proxy bypass attack. Then it give concrete attacks on Wang-Multi-Use-PRE scheme.

The Authors of “Optimizing the Computing of pairing with Miller’s algorithm” tries to do the basic loop of Miller's algorithm quicker with efficient arithmetic this by using Non Adjacent Form (NAF) and the window NAF (NAFw) instead of the binary form of the key in the original Miller's algorithm. It show how this improvement can reduce the number of addition steps by 1/6 in the NAF representation or 1/2(w+1) in the NAFw where w is the size of the window in the NAF.

Paper “High Payload and Secure Steganography method based on Block Partitioning and Integer Wavelet Transform” presents high volume payload and secure steganography technique based on integer wavelet transform. The cover image is partitioned into 8x8 non-overlapping blocks, then each transformed block partitioned into two subsets and secret message is embedded in proper subset. To achieve higher security, Haar wavelet transform is applied to the secret message before embedding it.

The paper “Predicting Terroristic Attacks in Urban Environments: An Internet-of-Things Approach” introduce a blueprint Internet-of-Things architecture for predicting terroristic attacks. The architecture allows Law enforcement agencies to exploit multiple data sources, (including SIGINT, OSINT and HUMINT) towards acquiring information associated with
terroristic action, while at the same time providing powerful reasoning capabilities towards transforming raw events into meaningful alerts.

The paper “Securing Bluetooth Communication with Hybrid Pairing Protocol” proposed a hybrid pairing protocol based on Diffie-Hellman Key Exchange protocol, MD5 and Hummingbird-2 to improve the level of security of Bluetooth communication. The developed hybrid pairing protocol adopted the DH Key agreement protocol to securely compute both parties’ shared secret key. MD5 hash function is used to solve the problem(s) caused by having a short PIN. This mechanism is integrated with the Hummingbird-2, a lightweight encryption algorithm, to further strengthen the pairing mechanism and at the same time, making it suitable for devices that has limited processing power and memory.

In the paper “Study on Enhancing Vulnerability Evaluations for BYOD Security”, focus on the private and confidential corporate information accessed from the attacker. It proposes the network model applying multiplicative security to test using the simulator, and then prove the safety by attack scenarios in BYOD environments. Especially in BYOD workplace, users as work tools can access sensitive corporate information from public areas. BYOD security challenges for corporate information are becoming more and more of a concern.

Paper “Research and Implementation of an Integrity Video Watermarking Authentication Algorithm” proposed the integrity video watermarking authentication algorithm based on DCT coefficients. Because of the characteristic of vulnerable to interference for high-frequency DCT coefficients, it use the relationship between the average energy of the high frequency coefficients and the energy of every the high frequency coefficients and Substitution cipher to beneficiate the Image Watermarking.

In the paper “A Study on the Improvements of Information Security Management System for Environment Education Institutes”, presents a variety of serious security incidents occur and appropriate educational environment to develop information security management system model. Applying the learning environment to enhance the level of data protection and information security management and direction of efforts to find ways to improve the model for improvement to propose.

The paper “Robust online filter recommended algorithm based on attack profile” analyzes the statistical features of the nearest neighbors of target users before and after attack. Design a kind of Attack Profiles online filter to attack the target user profile from the nearest neighbor filter on the basis of the work of the group effect on the attack profiles. And this filter improves the user-based recommendation algorithm nearest neighbor selection strategy, thus proposes the Collaborative Recommendation algorithm based on Online Filter for Attack Profiles (CROFAP).

The Authors of “Iris Feature Extraction based on Haar Wavelet Transform” propose an efficient algorithm for iris feature extraction based on 2D Haar wavelet. Firstly, the iris image is decomposed by the 2D Haar wavelet three times, and then a 375-bit iris code is obtained by quantizing all the high-frequency coefficients at third lever.

Paper “Shilling Attack Detection Algorithm based on Genetic Optimization” takes the group effect attack profile as the breakthrough point to construct the attack profile groups and the corresponding genetic optimization objective function of quantitative measure of the effects,
and prove that the maximum value of the objective function in the ideal state marks the optimum detection effects in ideal situation. On this basis, the combination of genetic optimization process will be adaptive parameter posterior inference and objective function, and proposes the Iterative Bayesian Inference Genetic Detection Algorithm (IBIGDA).

In the paper “Secure DRM Scheme Supporting Dynamic Authorization Using Attribute-Based Encryption”, propose a secure DRM scheme supporting dynamic authorization, which first encrypts content with content encryption key (CEK), and then protects CEK based on distributed attribute-based encryption. At last encrypted CEK will be packaged and distributed with encrypted content, which eliminates independent key management and reduces the burden on the DRM server. In the scheme, user is labeled with a set of attributes and CEK is associated with access policy, only the user whose attributes satisfy access policy of content can recover CEK, which also achieves fine-grained access control. Moreover, to improve Muller et al.’s DRM scheme, the scheme achieves dynamic authorization by adding action control in the license, while the action control is related to user’s payment.

The paper “Survey on reversible data hiding techniques” aims to present a survey on traditional data hiding techniques which are mainly based on reducing the embedding distortions. With the fast improvement of multimedia technologies and the rising attractiveness of the internet, information or data hiding methods have become more and more extensively applied to achieve authentication. Data hiding methods are ways of embedding additional messages into host signals by modifying their original contents without introducing perceptual changes.

The Authors of “Privacy Preserving Three-party Authenticated Key Agreement Protocol using Smart Cards” proposed three party authenticated key agreement (3PAKA) protocols to answer this question, which allows two parties to agree a new secure session key with the help of a trusted server. Recently, Yang et al. proposed a provably secure 3PAKA protocol. However, this paper finds out Yang et al.’s protocol has a security weakness against password guessing attack and two lack properties in authentication for password updating phase and privacy preserving. Furthermore, it propose anew privacy preserving 3PAKA (P_3PAKA) protocol using smart cards to solve the security problems in Yang et al.’s protocol. It provides user anonymity and un-traceability by adopting dynamic identifier depending on each session’s nonce.

Paper “Research on the Security based on Utility Theory in Cloud Computing Environment” focuses on the research of optimizing the safety and utility, proposing safety policy optimized model in cloud computing environment based on stochastic programming theory, building mathematical models which are on the basis of ensured data security to enhance the users’ utility, model analysis and optimization, and ultimately get the best optimized configuration of security policy in the cloud computing environment to guide the formulation and dynamic adjustment of access control policy in cloud computing environment, and to meet the users’ requirements, such as response time, resources availability and other utility requirements.

In the paper “Defending Against sybil-attacks in Peer-to-Peer Networks”, present a novel system to defend against Sybil attacks. The direct and indirect transaction protocols limit the number of service units that a node can obtain. Furthermore, it designs a dynamic reputation ranking algorithm for the indirect transaction protocol. Combining these two, a node with a high priority has more probability of obtaining service. The system does not try to prevent
users from creating multiple identities, but they cannot gain extra profit from doing so. It achieves a provable performance and overcomes the limitation of current social network-based defenses.

The paper “A Study on Behavioral Intention of Sharp(#) Mail Potential Users Focused on Non-Repudiation Function” aims to provide data and implications in which theories can be used in business by drawing a conclusion that can invigorate Sharp(#) Mail from a theoretical perspective through analysis on individual-targeted acceptance factor for individuals’ Sharp(#) Mail. Unified Theory of Acceptance and Use of Technology (UTAUT) was conducted for the study, which has much used in the research on users’ acceptance factor recently. For the subject of study, data were collected through the questionnaire survey developed to measure the use intention targeted for potential users who have an intention to use Sharp(#) Mail, research models and hypotheses were developed by using the PLS Path Modeling Approach to verify research hypotheses, and statistical analysis was conducted by using SMART PLS 2.0 analysis tool.

The paper “Preventive Maintenance Model Analysis Based on Condition” firstly constructs the full life cycle model with four-state of the devices, and then simplified it into three-state model based on some practical considerations. On the basis of it, the paper analyzes its reliability operation characteristics under diverse maintenance models such as the proactive maintenance based on CBM, the proactive maintenance based on TBM, and the passive maintenance, and the redundant maintenance scheme, and computes its desired maintenance cost and the investment payback period. The computing results show that the investments payback period is the shortest of the proactive maintenance rule based on CBM, and the one based on TBM comes second, and the one based on passive maintenance comes third, and the one of the redundant management model is the inferior.

July, 2014

Jemal H. Abawajy, Deakin University, Australia
Prof. Bharat Bhargava, Professor in Department of Computer Science at Purdue, USA

Editors of the July Issue on
International Journal of Security and Its Applications