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 19 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.

In the paper "Study on Intrusion Detection Policy for Wireless Sensor Networks", an intrusion detection policy is proposed for wireless sensor networks. It monitors the communication between neighboring nodes and finds those nodes that are not working normally. Some general rules are defined to detect such nodes called compromised nodes.

Paper "Efficient Assessment and Evaluation for Websites Vulnerabilities Using SNORT" investigated in details several examples of SNORT rules and how they can be tuned to improve websites protection. Practical methods were demonstrated to design and implement those methods in such ways that can show to security personnel how effectively can SNORT rules be used.

In the paper "Face Tampering Detection from Single Face Image using Gradient Method", an effective novel approach of detection and classification of real face image from tampered face image based on second order gradient is proposed in this paper. The intended purpose of proposed approach is to endorse the biometric authentication, by joining the vitality awareness with Facial Recognition Technology (FRT). The proposed method requires only one face image without requirement of additional equipment and easier to implement into existing face recognition technique. For this purpose, real (from own database and some publically available standard database) and tampered (own prepared databases of dummy, color imposed and masked faces) face image database are used here for verification and validation of our assertion.

The paper "Secure Model for Educational Resources" defines identity federation as a technology which enables the identity information to be trustily transferred across autonomous security domains. Shibboleth Federation is considered to trust logging process between different web educational resources, Fully Global log-out is not addressed by Shibboleth. In this Paper, Authors address Fully Global Log-out with a cached version of content as an off-line content, and enforce user to re-login for the new request after global logout. The paper modifies and utilizes the Shibboleth IdP source code to achieve securing model for web educational resources.

The Authors of "Classification of Malicious Domain Names using Support Vector Machine and Bi-gram Method" discusses that everyday there are millions of domains registered and some of them are related to malicious activities. Recently, domain names have been used to operate malicious networks such as botnet and other types of malicious software

(malware). Studies have revealed that it was challenging to keep track of malicious domains by Web content analysis or human observation because of the large number of domains. Legitimate domain names usually consist of English words or other meaningful sequences and can be easy to understand by humans, while malicious domains are generated randomly and do not include meaningful words or are not otherwise readable. Recently, a classification method has been proposed to classify malicious domain names. They used many features from DNS queries, including some textual features. However, it seems difficult to collect and maintain those data. The contribution is that, by using only domain names we could achieve better classification results, thus showing that domain names themselves contain enough information for classification.

Paper "A Secure and Anonymous Electronic Voting Scheme Based on Key Exchange Protocol" presents a discussion regarding voter anonymity and voting correctness which are important issues for electronic voting mechanisms. Compared electronic voting with traditional 1elections, an electronic voter is able to cast his/her ballot through the Internet in any place and at any time if he/she can access the network. Therefore, convenience and mobility make electronic voting become more and more popular and electronic voting can be adopted in the real world with higher feasibility. Recently, Chang and Lee presented an electronic voting (e-voting) scheme based on the blind signature and the Diffie-Hellman key exchange methods for ensuring voter anonymity and performance efficiency. They claimed that numerous essential requirements of general electronic voting can be ensured in their e-voting scheme. Unfortunately, we found that Chang-Lee's e-voting scheme suffers from susceptibility to security attacks and some critical security requirements of their e-voting scheme may be compromised. To prevent security weaknesses of Chang-Lee's e-voting scheme, in this paper, an improved version on their e-voting scheme is proposed that not only keeps the merits of Chang-Lee's e-voting scheme but also enhances the security of their e-voting scheme.

In the paper "Algorithms for Automatic Analysis of SELinux Security Policy", Authors discuss about the configuration of security policies which is an important but complicated work for running of secure operating systems. On the one hand, completely correct and consistent configuration is the necessary prerequisite for secure and credible system operation. On the other hand, errors and bugs are incidental anywhere within configuration at all time. Algorithms for automatic analysis of SELinux security policy are studied in this paper. Based on an improved analysis model similar to SELAC model, both algorithms for validity analysis and integrity analysis are designed. So that any access relations among subjects and objects with specified security contexts can be identified correctly by using the former algorithm. And all rules that could potentially influence integrity of subjects and objects can be detected based on the latter algorithm.

The paper "Security Analysis and Improvements of a Password-Based Mutual Authentication Scheme with Session Key Agreement" presents a discussion about a password-based authentication schemes have been widely adopted to protect resources from unauthorized access. In 2008, Chang-Lee proposed a friendly password-based mutual authentication scheme to avoid the security weaknesses of Wu-Chieu's scheme. In this paper, Chang-Lee's scheme was demonstrated that it is vulnerable to user impersonation attack, server masquerading attack, password guessing attack, and insider attack. An improved scheme to overcome the security weaknesses of Chang-Lee's scheme was proposed, even if secret information stored in the smart card is revealed.

The paper "Selective Timestamp-Nonce Based Authentication Scheme" aims to improve an efficient and complete remote user authentication scheme and propose an adaptive timestamp-nonce based authentication scheme using portable storage devices. Compared with other smart card-based, timestamp-based and nonce-based schemes, our scheme achieves more functionality. The new importance merits are: An adaptive timestamp-nonce structure is proposed; portable device stores authentication data not only smart card; all transactions through non-secure channel, especially in the registration phase, and batch of portable storage devices is issued. Besides, the basic merits include a dictionary of verification tables is not required to authenticate users, users can choose their password freely, mutual authentication is provided between a user and the remote system, the communication cost and the computational cost are very low, a user can update their password after the registration phase, a session key agreed by a user and the remote system is generated in every session and the serious time synchronization problem are solved.

The Authors of "Noise Resistant Identification of Human Iris Patterns Using Fuzzy ARTMAP Neural Network" proposes an efficient iris recognition system that employs circular Hough transform technique to localize the iris region in the eye image and cumulative sum based gray change analysis method to extract features from the normalized iris template and also fuzzy ARTMAP neural network to classify the iris codes.

Paper "Design of Internal Traffic Checkpoint of Security Checkpoint Model in the Cloud Computing" proposed design of internal traffic checkpoint in security checkpoint model for preventing security threats. The architected security checkpoint model is a system that performs firstly check process on all incoming traffic from outside network. And it identifies almost threats and prevents them for protecting a cloud computing resources. The security checkpoint model consists of three components such as incoming traffic checkpoint, internal traffic checkpoint, and host-based threat checkpoint. The proposed model checks the safety of incoming traffic and binary file, and tracks traffic including threat factors. And it also judges threat traffics on system and storage. This paper focused on structure, inspection procedures and functions of internal traffic checkpoint. Internal traffic checkpoint is important because it blocks threat traffic into internal network and ensures stable and reliable traffics.

In the paper "A New Data Aggregation Scheme to Support Energy Efficiency and Privacy Preservation for Wireless Sensor Networks", because a sensor node has limited resources, such as battery capacity, data aggregation techniques have been proposed for wireless sensor networks (WSNs). On the other hand, the provision of efficient data aggregation for preserving data privacy is challenging issue in WSNs. Existing data aggregation methods for preserving data privacy are CPDA, SMART, Twin-Key based method, and GP2S. However, they have a main limitation that communication cost for network construction is considerably high. To resolve the problem, Authors propose a privacy preserving data aggregation scheme based on Hilbert curve for WSNs. For data aggregation, a tree-based network structure is utilized which minimizes communication among sibling sensor nodes for network construction. A Hilbert curve technique to preserve data privacy is adpated. Because the sending data is encrypted by using a unique Hilbert value, it is very difficult to trace a real value even though attackers overhear the sending data.

Paper "Secure Video Transmission on Smart Phones for Mobile Intelligent Network" deals with video data delivery that comes up problems of the content ownership and the privacy, and thus protecting the video data becomes important in mobile network. With the

standardized protocol defined by AES-CCM, the need is to implement communication infrastructure for a next-generation mobile computing and intelligent system, i.e., Smartphone, evaluating security parameters (*e.g.*, CP (Control Parameter), UP (Unit Parameters) and standardization it's a challenging task. The details provided in this paper are used to design a CP based secure wireless video data transmission, on basis of AES-CCM for privacy issues, considering the security level with MAC overhead.

In the paper "Industrial Espionage and Police Investigation", Author presents a discussion that Industrial espionage has been worsening. To control industrial espionage requires new and stronger countermeasures. Among law enforcement agencies, the police are primarily responsible for preventing and controlling industrial espionage in terms of size and covering area. However, the police have many problems to be solved. The police have few experts on industrial espionage. The lack of budget and insufficient equipment contribute to hinder effective investigation. The lack of coordination among the investigation agencies and the absence of international cooperation system are also regarded as the problems to be solved. For the effective investigation for the police, therefore, it is necessary to train experts on industrial espionage. The special recruitment of outside specialists could contribute to improve the level of police investigation. Securing budget and cutting edge equipment are indispensable for effective investigation. Finally, the police should design a strategy to prove guilty and to prevent the concealment of the illegal gains from industrial espionage.

The paper "A Study on Performance Evaluation for Security Test Laboratory" studied performance analysis on the security test support project. In detail, the business flow of security product development activities was analyzed to measure performance of the facility and equipment project for quality verification of security products. In addition, multidimensional performance analysis was carried out empirically by applying it to a theoretical measurement model.

The Authors of "Security Requirements for the Medical Information Used by U-Healthcare Medical Equipment" aimed at the development of security test methodology for u-health medical devices and proposed the standard and specification to secure medical information security. For the purpose, first, the scope of u-health medical devices was defined and categorized its physical and operational types. Second, security core technologies were selected that can be applied to u-health medical device in three aspects such as administrative safeguard dealing with operator, policy, document, system and user education, physical safeguard dealing with control of entrance and exit, screen or shared instrument, and technical safeguard dealing with computer system-related technological elements. Lastly, each security core technology was assigned to each physical and operational types of u-health medical devices and relative significance of which was determined. The guideline containing the developed security core technology and test methodology for u-health medical device would be utilized for the enhancement of security level in the design of u-health medical devices and setting the authentication standard for authorization process for security in Korean Food and Drug Administration.

Paper "A Study on the Live Forensic Techniques for Anomaly Detection in User Terminals" deals with digital forensics techniques that have been used to analyze system intrusion incidents traditionally are used to detect anomaly behavior that may occur in the user terminal environment. Particularly, for the method to analyze user terminals, automated live forensics techniques that are used as supporting tool for malicious code (malware)

detection. A way to take advantage of the live forensic techniques for the anomaly detection of malware was suggested.

In the paper "Next Generation Electronic Record Management System based on Digital Forensics", due to technological advancement, it is very easy to generate electronic records within short period of time and with little effort. However, the challenge is to preserve electronic records for long period of time without losing their integrity and authenticity. This is critical problem because most of our day to day activities are dependent on the information we get from Electronic Record Management System (ERMS). The trustworthiness of electronic record is dependent on ERMS. Therefore, ERMS has vital role in keeping electronic record for long term without losing its trustworthiness. In this paper, a novel approach was proposed for next generation ERMS that alleviates these challenges.

The paper "Linear Relationship between Reported Discretional Expenditure and Sales Amount – Empirical Approach with IT Related Industry" discusses about financial studies that assume linear relationship between discretional expenses and sales amount. Also previous researches insist that industry having shorter product cycle has strong relationship between them. Linear relationship between them based on financial reports during 2000-2011 of appearing companies in top 100 firms based on advertising amount were investigated. Food product manufacturing and electronic component manufacturing industry representing industry were chosen with short product cycle and IT industry.

January, 2013

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

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