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 39 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 “An Empirical Study to Compare the Performance of some Symmetric and Asymmetric Ciphers” presents empirical results obtained from Java implementation of Elliptic curve Cryptosystem (ECC) as an asymmetric block cipher algorithm and a set of symmetric block cipher algorithms namely Triple-Data Encryption Standard (T-DES), Advanced Encryption Standard (AES), and Blowfish. Performance evaluation based on CPU execution time is presented under WinXP and Linux.

Paper “Key Distribution using Double Keyed-hash Chains for Wireless Sensor Networks” proposes an effective key predistribution scheme using double keyed-hash chain schemes. In the proposed scheme, there are two key pools: upward key pools and downward key pools, and the key ring in each sensor is picked from these two key pools. The proposed scheme is analyzed based on connectivity, resistance against attacks, memory consumption and communication overhead. Comparing with the EG scheme and the q-composite scheme, the scheme performs better in terms of network resilience to node capture with little additional overhead cost.

In the paper “Improving the Detection of Malware Behaviour Using Simplified Data Dependent API Call Graph”, proposed a malware detection system based on API call graph. Each malware sample is represented as data dependent API call graph. After transforming the input sample into a simplified data dependent graph, graph matching algorithm is used to calculate similarity between the input sample and malware API call graph samples stored in a database. The graph matching algorithm is based on Longest Common Subsequence (LCS) algorithm which is used on the simplified graphs. Such strategy reduces the computation complexity by selecting paths with the same edge label in the API call graph. Experimental results on 85 samples demonstrate 98% detection rate and 0% false positive rate for the proposed malware detection system.

The paper “A Mutual RFID Security Protocol for Wireless Reader” projected mutual RFID authentication protocol for wireless reader that can meet lightweight encryption function structure protection this protocol only requires $O(1)$ work to identify and authenticate a tag in the server. The security properties of the proposed protocol are analyzed as well by comparing with the related RFID authentication protocols.

The Authors of “A Simple and Fast Technique for Detection and Prevention of SQL Injection Attacks (SQLIAs)” proposed a new technique based on static analysis and runtime validation
for detection and prevention of SQLIAs. In this technique user inputs in SQL queries are removed and some information is gathered in order to make the detection easier and faster at runtime.

Paper “A New Fast and High Performance Intrusion Detection System” build a fast and high performance hybrid hierarchical intrusion detection system called NFPHIDS that possesses the following characteristics: have a short training time, detect the low frequent attacks, give a high detection rate for frequent attacks, and give a low false alarm rate. NFPHIDS contains two levels. The first one includes four fast classifiers Random Forest, Simple Cart, Best first decision tree, Naïve Bayes used for their excellent performance on the detection of respectively Normal behavior and DOS, Probe, R2L, and U2R. Only five outputs of the first level are selected, and used as inputs of the second level that contains Naïve Bayes as final classifier.

In the paper “A Novel Multi Scale Approach for Detecting High Bandwidth Aggregates in Network Traffic”, proposes a two stage wavelet based statistical detection algorithm to calculate self similarity for the detection and visualization of anomalous traffic in the computer network traffic. The computer network traffic under normal circumstances exhibits long range dependence and when under attack it deviates from its behaviour. Along with the detection of an attack its point of presence is also identified. The detection algorithm was tested on simulated patterns of flooding attacks, pulsating denial of service attacks and flash crowds under low, moderate and heavy traffic. The tested scheme was then validated with KDD based publicly available dataset.

The paper “A Robust Behavior Modeling for Detecting Hard-coded Address Contained Shellcodes” proposed a robust run-time heuristic for detecting this type of shellcode. The objective is to augment the collection of the existing run-time heuristics.

The paper “Implementing Database Methods for Increasing the Performance of Intelligent CCTV” is written for intelligent CCTV (Closed-Circuit Television) which has been important in the aspect of industrial value and social security these days. Because the intelligent CCTV can identify behavior and object automatically, and it has been used extensively. With spread use, the performance of the intelligent CCTV has been important. But a standard method to measure the performance of the intelligent CCTV is absence, therefore this paper is described about methods for implementing and measuring of the intelligent CCTV performance.

The Authors of “A Novel Method to Avoid Malicious Applications on Android” introduced with analysis of the method to prevent an installation of malicious applications using permissions using Maximum Severity Rating (MSR) classification. Then, the method to enhance an ability to perceive warning signs in the procedure of an application installation and comparison of its effectiveness with existing method is introduced. Overall, the processes assist the users to make a better decision with detailed information.

Paper “Efficient mCoupon Authentication Scheme for Smart Poster Environments based on Low-cost NFC” proposed a secure mCoupon authentication scheme that is protected against illegal use in smart poster environment based on low-cost NFC to using limited resources.

The paper “Content Reuse Prevention Scheme to Prevent Privacy Invasion of Social Network Service” planned a content reuse prevention scheme based on digital right management
(DRM) techniques to solve the problem of the unwanted reuse of stored content in a malicious user’s “Temporary Internet Files” folder.

Paper “Experimental Study of DDoS Defense System for Web Service” proposed several defense mechanisms against DDoS attacks. However it is not easy for a security manager to select solutions suited for his service environments. Under the respect, this paper is intended to classify DDoS defense systems based on the functional design method. Also it shows various experimental results of DDoS defense systems by using the proposed classification of defense systems and performance metrics.

In the paper “Policy Direction of QoS Interworking and Management among Service Providers for Broadcast-Communication Convergent”, analyzed the related standard documents and cases of other nations to set up a classification model of providers and scheme for QoS management among providers. With the results of the analysis, it provides a policy direction for the QoS interworking and management among providers in South Korea.

The paper “A Logistic Neural Network Approach to Extended Warranty Claims” uses model based on the knowledge of traditional diffusion theory as well as artificial neural networks. Additionally, it integrates the two into a hybrid model in order to study extended warranty growth. A count of greenery warranty can be used as a reliable measure of extended warranty growth in all the models. The study demonstrates that a logistic Neural Network model, if properly calibrated, can create a very flexible response function to forecast the extended warranty claims. The logistic neural network successfully modeled both the usual and environmental influences in the warranty data, while the traditional formulation could only model the usual warranty claims. Logistic, artificial neural network and logistic neural network analysis are carried out on the green warranty presenting to a warranty repair department.

The Authors of “Vehicle License Plate Recognition Based on Hierarchical Approach” introduced hierarchical approach and overlapped partitioning technique in order to accurately detect the various sizes of vehicle license plates which are included in input image. The proposed approach firstly attempts the license plate detection for entire image. If detection is failed, the image is partitioned into 3 overlapped rectangular areas and the license plate detection is attempted again. If detection is failed again, the image is partitioned into 7 overlapped rectangular areas and license plate detection is attempted. The method to use for detecting license plate in each step is the edge-based projection technique.

Paper “Audio Watermarking by Coefficient Quantization in the DWT-DCT Dual Domain” propose an effective and robust audio watermarking algorithm that employs both the discrete wavelet transform and the discrete cosine transform. The algorithm involves, first, pre-processing of the binary watermark image and then embedding it into the original audio by quantization of coefficients.

The paper “Intrusion Detection Ensemble Algorithm based on Bagging and Neighborhood Rough Set” presents a new ensemble algorithm to improve intrusion detection precision. Firstly, it generates multiple training subsets in difference by using bootstrap technology. Then using neighborhood rough sets with different radiuses to make attribute reduction in these subsets, obtained the training subsets with greater difference, while Particle Swarm Optimization is used to optimize parameters of support vector machine in order to get base
classifiers with greater difference and higher precision. Finally, the above base classifiers were integrated by weighted synthesis method.

The paper “Secure Communication based on a Fractional Order Chaotic System” studied the fractional order chaos of PMSM system. The process that PMSM system change into chaos with the variation of fractional order is revealed by bifurcation analysis. According to the stability theory, the stability of equilibrium point of PMSM system is analysed. In the same way, some representative track point of the system is analysed and by doing this the essence of chaotic operation is revealed. Then the adaptive synchronization of PMSM system is studied. A controller with an adaptive changing rate is designed and its feasibility is theoretically proved. Introduced the implementation method of chaotic masking.

In the paper “Network Security Threats Situation Assessment and Analysis Technology Study”, presented an evaluation method that based on dependency analysis. First, dependency relationships among services are identified from the management information of operating system and the monitoring records of network communication. Afterwards, the direct threats imposed by attacks on services and the indirect threats that transfer along dependency relationships are evaluated, and the threats that come from multiple attacks are composed by means of nonlinear composition. Finally, according to threat degrees and service values, the threat situation of the whole service architecture is evaluated.

Paper “Construction of Trusted Wireless Sensor Networks with Lightweight Bilateral Authentication” presented a lightweight authentication model for wireless sensor networks composed of a key management and an authentication protocol. It is based on the use of trusted primitives with very low computational requirements, which obtains better results than other proposals in the literatures.

In the paper “An Improved Algorithm of Elliptic Curve Cryptograph”, studied the fast implementation of elliptic curve cryptosystem key algorithms, namely, Scalar Multiplication. The limitation of the traditional fixed point comb method is analyzed, and on the basis of the study improvement strategy of fixed-base comb algorithm of this proposed, thus the speed of the whole system can be improved. Through the analysis of Power Analysis Attacks, and on the basis of comb fixed point method, resist power analysis attack methods is analyzed, and the further corresponding improved algorithm is put forward. Through the performance comparison analysis, the improved algorithm can get higher power analysis attack resistance.

The paper “Attack Graph Algorithm in the Application of Intrusion Detection System” puts forward the attack graph which is based on intrusion detection method in order to discover the network vulnerability timely and solve the very serious problems of network security. The method uses the generation global network attack graph algorithm to build network initial attack graph, and call attack graph optimization algorithm to remove global attack graph unreasonable path, and achieve the goal of simply attack graph. Finally, management personnel get the basis which is computed nodes in each state attack graph algorithms degree of loss to optimize the network security.

The Authors of “A Heuristics-based Static Analysis Approach for Detecting Packed PE Binaries” present a static heuristics based approach for the detection of packed executables. It presents 1) the PE heuristics considered for analysis and taxonomy of heuristics; 2) a method for computing the score using power distance based on weights and risks assigned to the
defined heuristics; and 3) classification of packed executable based on the threshold obtained with the training data set, and the results achieved with the test data set.

Paper “Preventing and Detecting Plagiarism in Programming Course” analyzes and expatiates the reasons and the methods about the code’s plagiarism, and thinks there are two phases in preventing this plagiarism: one is preventing plagiarism from occur, the other is to detect cases of plagiarism when the preventative measures fail. Preventing plagiarism methods mainly include the valid course assignment design and to forbid the electronic copy. This paper describes a code’s editor software which has been implemented use Java. When the preventative measures fail, this paper describes an automatic tool to help instructor find the suspicious targets. These phases’ aim is to cut down the plagiarism and improve the ability of the student’ programming.

In the paper “An Adaptive Method for Source-end Detection of Pulsing DoS Attacks”, presented an adaptive method for source-end detection of PDoS attacks. This method requires little knowledge of the network traffic except a loose symmetry between the outgoing packets and the incoming packets. Three distinct features of this method are emphasized. Firstly, no assumption is made on the distribution of the traffic samples. Secondly, it succeeds in implementing a self-adjusting detection threshold, which makes it adapt to various traffic conditions. Thirdly, it reacts quickly to the end of the PDoS attacks.

The paper “Platforms and Applications in Hardware Security: Trends and Challenges” introduces a few research studies being conducted that are using multicore embedded systems, highlighting the challenges and questions relevant to R&D (Research and Development) in computer systems architecture, focusing on design aspects and optimization of embedded systems that needs to run security solutions or cryptographical algorithms using hardware acceleration, aiming for good performance, code optimizations, and the lowest energy consumption. Another aspects are the design of dedicated processors for specific purposes, multicore systems and GPUs for security solutions and specific applications requiring high performance, with the possibility to work with FPGAs or embedded platforms with embedded multicore paradigm.

The paper “Access-control-based Efficient Privacy Protection Method for Social Networking Services” proposed a method for the efficient protection of privacy in SNS based on access control. There has been a recent surge in the popularity of social networking services (SNSs) and SNSs have grown rapidly, as has the variety of information shared through SNSs. However, SNSs raise concerns about the security and privacy of users because the information written by the user might be exposed in the SNS. Many studies have addressed this issue, but previous research has lacked methods that can be applied efficiently in the SNS environment.

The Authors of “Security Management Architecture for Secure Smartwork Center” proposed Security management architecture for the construction of a secure smartwork center. Since smartwork can provide a flexible and convenient mode of work for employees, many companies are preparing to adopt smartwork systems for their work environments. In addition, many companies are supporting a “SmartWork Center” to increase the staff’s work efficiency. However, in a smartwork center, most users use public devices and work in open network environments. As a result, there can be security vulnerabilities such as the leakage of secret data, invasion of privacy, viruses, and the spread of malware.
Paper “Trust-Based Clustering in Mobile Ad Hoc Networks: Challenges and Issues” presented numerous trust-based clustering schemes to protect the network clustering from security attacks. Analyzing the existing trust-based clustering solutions, the researchers illustrated their primary features and properties in this paper and mainly discussed about the trust management mechanisms which are integrated in each trust-based clustering solution. Besides it was illuminated how trust and reputation are used in the cluster formation and maintenance phases.

In the paper “A Study on Differential User Authentication Scheme based on Client in Home Network”, proposes the scheme for differential user authentication based on client in home network at a remote place. The scheme supports the convenience and strengthens the security by using the unique value of the registered client. In case of using the unregistered client, it protects the authority accessing the home network via the method strengthening the user authentication by using the security card.

Paper “A Multi-Stage Fingerprint Recognition Method for Payment Verification System” proposes a method to utilize the strengths of the Multi-Stage Fingerprint Recognition Method for Fingerprint Payment Verification System. The example of the utilization of the credit card payment is the model business of fingerprint verification credit card payment applied for three months in large domestic marts, to discuss the possibility to settle the non-medium credit trading by the biometric technology and the applicability to the financial services.

In the paper “Relative Importance Analysis of inter-evaluation items in Korean IS Standard Audit Checklist Using Decision making Techniques”, applied AHP and MOGSA decision making techniques and drew weights and priority of inter-items in standard audit checklist. Derived weights and priority can be used as a basis to modify and change evaluation items in standard audit checklist. The same priority has been obtained from used two methods and two decision makers’ groups. As a result, it was demonstrated that derived priority has high reliability.

The paper “A Novel Image Encryption Using Arnold Cat” 3D Arnold cat map can be applied in image encryption, and it has more security and better effect. However, its period is fixed. The original image will be returned to itself if iterating some times. On the basis of 3D Arnold cat map, it presented an algorithm of image encryption which separates the original image to many same blocks and no period.

The Authors of “An Improved Overlap-Key-Sharing Key Management Scheme for Wireless Sensor Networks” proposed an improved Overlap-Key-Sharing key management scheme on the basis of Overlap-Key-Sharing (OKS) management scheme and the group-based model of Wenliang Du and Donggang Liu et. The management scheme has little storage consumption and good resilience against node capture. In this paper, it mainly do some analyses and evaluations on a basic random key pre-distribution scheme (E-G scheme) which is proposed by Eschenauer and Gligor et and the improved Overlap-Key-Sharing key management scheme.

Paper “An Encryption Method for QR Code Image Based on ECA” proposed a two-dimensional code encryption and decryption method based on Elementary Cellular Automata state rings in order to improve security performance of the information stored in two-
dimensional Code (Quick Response Code). Cellular Automata can simulate complex phenomena just using simple dynamical system. In addition, Cellular Automata and cryptography have a lot of similarities such as diffusivity and integrated chaos. Based on this feature, the method uses the Cellular Automata to encrypt and decrypt QR code binary image with the following parameters: the length is 8, the boundary condition is cyclic boundary condition and \{0, 1\} is the state space.

The paper “Design of Active Frequency Selective Surfaces for the RCS Reduction” presents a novel three-dimensional active frequency selective surfaces loading a varactor diode to achieve electrically controllable, by loading different values of paranoid voltage to control the variable capacitance diode. Simulation results show that the structure has excellent resonant characteristics in the range of 3.34GHz-1.59GHz, and has certain sensitivity for the change of the capacitance value, so it can achieve electrical controllable in the frequency band.

In the paper “Byte-index Chunking Algorithm for Data Deduplication System”, presents an algorithm and structure for a deduplication method which can be efficiently used for eliminating identical data between files existing different machines with high rate and performing it within rapid time. The algorithm predicts identical parts between source and destination files very fast, and then assures the identical parts and transfers only those parts of blocks that proved to be unique region. The fundamental aspect of reaching faster and high scalability determining duplicate result is that data are expressed as fixed-size block chunks which are distributed to “Index-table” by chunk’s both side boundary values. “Index-table” is a fixed sized table structure; chunk’s boundary byte values are used as their cell row and column numbers.

The paper “Development and Analysis of an Information Security Learning Method using Situation-based Problems” proposed how to provide a customized learning and developed the corresponding information learning contents to bring tailored learning. Finally, It examined how learners feel about information security and whether the necessity of information security learning increases or not.

September, 2013

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

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