Abawajy, Jemal, Bhargava, Bharat and Xiong, Neal N. 2016, Foreword and editorial: International journal of security and its applications, *International journal of security and its applications*, vol. 10, no. 5, pp. v-xii.

Foreword and Editorial

International Journal of Security and Its Applications

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

This issue contains 33 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.

Paper "A Novel Information Fusion Model for Assessment of Malware Threat" proposed a novel information fusion model to quantitate the threat of malware. The model consists of three levels: the decision making level information fusion, the attribute level information fusion and the behavior level information fusion. These three levels portray special characteristics of malware threat distributed in the assessment model. Combined with the static analysis technology and real-time monitor technology, they implemented a framework of malware threat assessment. The experiment demonstrates that their information fusion model for malware threat assessment is effective to quantitate the threat of malware in accuracy and differentiation degree. In the end, they discussed several issues that could improve the performance of the model.

In the paper "Achieving Secure Deduplication by Using Private Cloud and Public Cloud", at the present time, cloud computing furnish large volume of area for storage of data as well as huge equivalent computing at affordable rate. Due to advantages of cloud computing it turn out to be widespread; extreme quantity of data can be stored on cloud. But, rise in size of data has raised numerous new obstacles. Deduplication is one of significant compression method of data for reducing carbon copy of replicating data that being used in cloud to reduce the volume of storage area and it utilizes less network bandwidth. Data Deduplication is the convergent encryption technique that has been projected to encrypt the data before it's been sent out that preserve the confidentiality of responsive data. For better data security, it makes the initial effort that officially point out the dilemma of authorized data Deduplication. There are numerous new Deduplication structures that provides authorized duplicate check in hybrid cloud structural design that acquire negligible overhead over standard operation.

Paper "Improving Unconstrained Iris Recognition Performance via Domain Adaptation Metric Learning Method" proposed a performance improvement method of unconstrained iris recognition based on domain adaptation metric learning to improve unconstrained iris recognition system performance in different environments. A kernel matrix is calculated as the solution of domain adaptation metric learning. The known Hamming distance computing by intra-class and inter-class is used as the optimization learning constraints in the process of iris recognition. An optimal Mahalanobis matrix is computed for certain cross-environment system, then distance between two iris samples is redefined.

Paper "On Privacy and Anonymity in Freenet System" reviews and summarizes the research progress of Freenet system by collating and analyzing relevant articles. They also analyze and compare the main ideas, the algorithm application as well as pros and cons of different articles surrounding different topics. In addition, they also tease out the development and the evolution trends of Freenet system in time order, and combined with

current network situation, they made reasonable proposals and prospects and draw scientific conclusions.

The article "Use of Silence as an Altered Approach for Speaker Recognition" presents an alternative approach and puts forth the experimental results of obtaining silence as a parameter to check if the pattern of pauses/silence for train and test files recorded for individual speaker match. The paper emphasizes the approach in which a paragraph is recorded for 8 speakers and used as train files. The duration of silence/pauses of the speaker in a paragraph are obtained. This silence obtained is compared with the silence obtained from test file the matching of pattern of the silences decides the identity of the speaker.

In the paper "An Analysis of Internet Censorship Circumvention Techniques", Since Internet was born, it has deeply influenced almost every aspects of people's life. However, at the mean time when people enjoy the convenience brought by the Internet, there is censorship existed every corner of the internet world. Censorship circumvention technique to protect people's communication against censors. During the past decades, anti-censorship techniques have a broad and extensive development, however not all of the censorship circumvention techniques have effect in circumvent the censors and there is still not a very useful and convenient technique to ensure the anonymity of internet communication. In this paper, they tried to analyze the current situation of censorship and anti-censorship techniques and give a comprehensive view on the censorship circumvention techniques and systems.

The study "Improving the Handoff Latency of the Wireless Mesh Networks Standard" proposed an improvement to the IEEE 802.11- based wireless mesh networks in terms of authentication latency. The current paper, proposes a new, easy, fast, and secure handover design. In addition to, a new security metric is presented, which is the ability of the authentication protocols to determine the identity of the users who make bad behaviors with a complete preservation to the privacy of the rest users. They can say that it's a very a difficult problem, due to the trade-off between the privacy and the non_ repudiation property. A formal authentication verification method is presented, using BAN logic analysis.

In the paper "An External Parameter Optimize Method for 3D Optical Measurement System", a simple and effective external parameter calibration and optimize method based on epipolar geometry for improving the accuracy and stabilization of 3D optical measurement system are present. First, the internal parameters of two cameras are calibrated using the planar calibration method. Then using the parameters as initial value calibrates the external parameter of the 3D optical measurement system in every view. Optimization result is computed through minimizing epipolar line error of the same pair of points in every view.

Paper "A XSS Attack Detection Method based on Skip List" presents a cross-site scripting attacking detection method, which is based on improved algorithm skip list. It can fulfill the rapid detection of cross-site scripting attacks by using some steps, for example, creating a skip list signature, detecting suspicious strings, marking attack vectors and so on.

The researcher in the study "Digital Image Watermarking Based On Joint (DCT-DWT) and Arnold Transform" has adopted a digital watermarking technique which operates in the frequency domain: a hybrid watermarking scheme based joint discrete wavelet transform – discrete cosine transform – (DWT-DCT). Its main objective is to test whether

this technique can withstand attacks (its robustness) and invisibility (its imperceptibility), achieved by taking DCT of the DWT coefficients of the LL mid-frequency sub-bands from its band. To ensure security, the secret code (watermark) is scrambled using the Arnold transformation which is embedded in the original host image; only gray-scale digital images are used. The results of this research reveal that the secret code (watermark) is strong enough against threats (noise).

In the article "Image Steganography in a Karhunen-Loeve Transform Optimization Model", in allusion to such problems as large perceptual distortion and high error rate caused by high image compression ratio in existing steganography technology in the information security field, an image Steganography based on Karhunen-Loeve transform optimization is proposed in this paper. Specifically, the iterative clustering algorithm is adopted for this method to solve the covariance matrix and the clustering mean value, and relevant values are adjusted for image segmentation; then, KLT algorithm is introduced to compress the image data and the least significant bit is adopted to replace the ciphertext data for data hiding. During information extraction, the reverse linear transformation operation and the original pixel matrix are adopted to obtain the effective hidden image information.

In the study "Network Information Security Situation Assessment Based on Bayesian Network", the situation of information security is difficult to be precise, autonomous and controllable. In this situation, the situation of the system is based on Fuzzy Dynamic Bayesian network. The model of situation awareness and situation estimation is constructed.

The term paper entitled "Evaluation of Flow and Average Entropy Based Detection Mechanism for DDoS Attacks using NS-2" talks about such solutions to combat DDoS attacks. Here, the flow entropy in combination with average entropy technique is used to detect an attack. It highlights how the loop holes of one technique are covered by the other, resulting in a considerable improvisation in the methods of how they deal with these attacks.

In the study "A New Collusion Attack Using Interpolation for Multimedia Fingerprinting", digital fingerprinting is a special digital watermarking technology that can deter legal user to redistribute multimedia content to others. With traitor tracing, it can detect illegal users who use multimedia content illegally. However, collusion attack can avoid some illegal users being detected. With different fingerprinted copies, collusion attack can produce a new colluded fingerprinted copy for get rid of the fingerprint information from the colluded copy, so digital fingerprinting technique should deter collusion attacks. In order to improve the performance of new digital fingerprinting technique in future, this paper presents a new collusion attack approach based on interpolation. The proposed interpolation collusion attack scheme comes from the idea of image fusion.

The paper "Effect of Anhydride Grafting Agent on Trap Levels of Low-Density Polyethylene" states that trap distribution of the low-density polyethylene(LDPE) modified by anhydride grafting agent was studied and the effect of grafting agent on the trap levels was analyzed by the method of Photo-stimulated Discharge in this paper. Different concentrations and types of same concentration of LDPE modified by anhydride grafting agent were measured by using continuous UV scanning. The results showed that different concentrations and types of grafting agent had effect on trap levels distribution of LDPE. The trap depth would decrease with the anhydride grafting agent content increasing and increase with its damaged condition increasing when anhydride grafting

agent was destroyed. Anhydride grafting agent are widely applied to the production and research of high pressure insulating polyethylene materials. The purpose of this paper is to elaborate the effect of anhydride grafting agent on the insulating properties of polyethylene material and explain the strongest binding capacity of anhydride grafting agent to space charge.

Authors of the paper "A Cybercrime Prevention Program based on Simulation and Quiz Game: Applying Item Response Theory for Effective Information Security Learning" develop a program with learning contents based on a simulation for preventing cybercrimes. Furthermore, they provide a quiz game to enhance the understanding of the cybercrimes. After learning through the quiz game, the learners can check and extend their knowledge of preventing the cybercrimes. Specifically, each learner can identify vulnerable cybercrime types and get the proper feedbacks for preventing them through the analysis of learner's own correct/wrong answers.

In the study entitled "Research on Wormhole Attack Detection Algorithm in Space Information Networks", wormhole attack is a coordinated attack that launched by two or more malicious node. With a high quality private link malicious node, attracted traffic, attacked routing protocol, destroyed network topology, has a great threat to space information network. They propose a wormhole attack detection algorithm based on abnormal topology and time delay in space information network and the algorithm is mainly composed of two phases: finding abnormal topology and getting the malicious node. According to the number of nodes which are mutually non-one-hop neighbors in the normal network and the abnormal topology in backbone get the suspicious neighbors. To confirm the fake link, uses the round trip time to detect suspicious neighbors. Sends warning messages to isolate false neighbors or malicious nodes to ensure the security of the network. Using the network simulation software NS2 analyses the performance of the detection algorithm.

Paper "Intrusion Detection Method based on Improved BP Neural Network Research" states that with the development of computer network technology, more closely the relationship between people and network.The current network security problem has also been gradually into the public's field of vision, actively carried out on the network intrusion detection becomes an important direction of the development of the network security technology.On the basis of the original BP neural network, this paper puts forward an improved algorithm, and applied to network intrusion detection. After the test, the method is better than traditional convergence, better performance.

Authors of the paper "Fast Detection of Copy-Move Forgery Image using Two Step Search Algorithm" proposed a new fast detection method of copy-move forgery image using two step search algorithm in the spatial domain. They proposed a new two step search algorithm for copy-moved forgery image detection. The performance of the proposed method is experimented on several forged images. Their two step search algorithm reduced 96.82% computational complexity more than conventional algorithms for copy-move forgery image detection. The block distortion measure (BDM) of the two step search algorithm is sufficient by 2 pixels checking points instead of 64 pixels checking points for exhaustive search in the not copy-moved forgery image regions. Most blocks of the images constitute not copy-moved forgery images. Therefore, they can reduce computational complexity more than conventional methods. They didn't use any exhaustive search method and frequency domain (ex. DCT, Wavelet Transform) to reduce computational complexity in this paper.

In the paper "Representation of Network Security Situation Elements Based on Cloud Model", aiming at efficiently aware the network security situation, they proposed a framework of Network Security Situation Awareness on the base of Cloud Model. With network security situation elements at the core, they modified the Cloud Model to a novel concept, situation cloud, which act as theoretical foundation in the transition between the qualitative and quantitative representation on situation elements.

In the study "An Improved Random Key Predistribution Scheme for Wireless Sensor Networks Using Deployment Knowledge", key management is the basis of many security mechanisms and services in wireless sensor networks (WSN). Random key predistribution scheme is widely considered as the most practical for WSN. However, this scheme faces the challenge that it cannot achieve the ideal security connectivity and strong resilience against node capture simultaneously. To address this limitation, an improved random key predistribution scheme using deployment knowledge is proposed in this paper. Firstly, sensor nodes are divided into different groups according to their location expected. And the key pool is grouped into key pool subsets accordingly. To realize the communication between adjacent groups, the corresponding key pool subsets have a certain degree of overlapping. For all keys, there is no limitation on key reuse. Neighboring nodes sharing q common keys will establish secure link with high probability. Moreover, their scheme inherits the advantage of q-composite random key predistribution scheme that it can maintain security even if some nodes are captured.

In the paper "A Study of Effective Defense-In-Depth Strategy of Cyber Security on ICS", the system of SCADA(Supervisory Control and Data Acquisition Security) used in electricity, water, petroleum and gas, transportation as well as manufacturing, is to collect scattered data and to monitor assets related as a centralized suppression system. ICS system, including current SCADA, is not isolated from outside, being connected with IT solution, and can operate equipment through broadband network, instead of accessing physically. Accordingly, the security accident of suppressing system can occur in the fields of antagonistic nations, terrorists, foundational facility invaders, natural disasters and ill-will or accidental actions. The security control examined in this study provides a defense-in-depth strategy which is applicable to the effective cyber security strategy regarding ICS to protect the confidentiality of information, zero defect, availability through the classification of control, operational control and technological control.

Paper "A Fast Detection and Recognition Algorithm for Pedestrian at Night Based on Entropy Weight Fast Support Vector Machine" states that in allusion to such problems as real-time requirement dissatisfaction and significant recognition difference caused by dimension difference existing in the imaging and recognition algorithm for pedestrian in dark scene, a fast head detection and recognition method for pedestrian at night based on fast support vector machine (FC-SVM) algorithm optimization and entropy weight is established in this paper according to relevant principle of statistics. Based on entropy weight, this method aims at improving the extraction process based on histogram gradient features in order to establish three-branch SVM for the deep recognition of pedestrian at night; meanwhile, FC-SVM algorithm is combined to optimize the recognition calculation overhead in order to ensure the real-time property of the recognition algorithm. Furthermore, the falsely detected pedestrians are evaluated on the basis of the head detection mode so as to improve pedestrian imaging matching accuracy. The simulation result shows that this method can not only effectively recognize FIR target of pedestrian at night, but also effectively adapt to such different application environments as urban and suburban areas on the basis of ensuring the real-time requirement for pedestrian recognition, thus presenting good practicability.

In the study “Intrusion Detection in Aviation Terminal Region Petri Net with Non-arc and Unchanged Library”, due to the complex structure and the large number of the running aircrafts in the application of the intrusion detection in terminal regions, the defense conflict dangers and the influence on aviation safety exist in such terminal region. Therefore, Petri net framework with non-arc and unchanged library is constructed in this paper to propose the terminal intrusion detection scheme. Firstly, the aviation operation structure of the terminal region is analyzed and the constraint model of the terminal region is constructed as the terminal intrusion detection basis according to Petri net model framework; secondly, the aviation constraint model of the terminal region constructed thereby and the principle of non-arc and unchanged library are adopted to establish the terminal intrusion detection control strategy, and the control decision is made according to the transition activation for the aviation instructions; finally, the experimental analysis of the practical cases shows that the proposed terminal intrusion detection scheme can effectively handle the terminal intrusion detection problem and reduce the workload of the controllers.

In the paper “Security Analysis Of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study”, various dimensions of VANETs including its emerging applications, security issues, challenges, security threats and the existing solutions proposed by the different researchers are studied. Also author reviewed various type of VANET simulator available and presented possible key research area of VANETs.

Paper “Simulation and Optimization Study on Layout Planning of Plant Factory Based on WITNESS” tells that the emergence of plant factory has solved great restriction problem of natural environment in the traditional agriculture. Therefore, it has been the research concentrate on the facility agriculture in recent years. However, the reasonability of factory's production process and layout determines quality of the product, production efficiency and economic benefits. This paper took Wuchang Jingtian Plant Factory as an example, analyzed the production process and layout and provided a corresponding improvement scheme which was verified by the WITNESS simulation software. An optimal solution was determined from the evaluation index of production efficiency, busy rate, production cycle etc.. Besides, the simulation analysis of production cost before and after the improvement verified the improved plant factory operation is effective and feasible. This improvement scheme not only improved efficiency of production system of the plant factory, but also reduced the operating cost.

The paper “The Research of AMI Intrusion Detection Method using ELM in Smart Grid” proposes an ELM-based intrusion detection method for AMI. They first filter and partition the malicious data, and then different types of invasion are effectively extracted. Finally, they can use Extreme Learning Machine(ELM) for detecting different attack types of malicious data. However, traditional machine learning algorithms such as Support Vector Machine(SVM), which results in a longer training time and poor performance, and moreover SVM is not applicable to multi-class problems. In theory, ELM can approximate any target continuous function and classify any disjoint rejoins.

The study “Improving Analysis Phase in Network Forensics By Using Attack Intention Analysis” aims to show the importance of reconstructing attack intentions in order to improve the analysis phase in network forensics. Intentions are identified through an algorithm called Attack Intention Analysis, which predicts cyber crime intentions by combining mathematical evidence theory and a probabilistic technique. In this paper, the attack intention model will be improved to present the motivation behind cyber crimes.

Paper “Application of Combined Positioning Algorithm of Volume Image Sequence on Mapping of Large Scale Topographical Map” proposed the combined positioning algorithm of volume image sequence, which is applied in large scale topographical map. Firstly, the observation equations of observable image sequence are analyzed, and the five different coordinates relating with space 3D coordinate of object can be calculated. Secondly, the combining positioning algorithm based the characteristics of hyperbolic curve and Kalman filter is put forward and the corresponding mathematical model is constructed.

In the paper “Research on Intrusion Detection Systems and Unknown Malcode Detection based on Network Behavior”, based on the analysis of malicious code detection technology and detection system, the author designs and implements an unknown malicious code detection system based on network behavior analysis. Test results show that the detection system can distinguish three kinds of ARP attack; it can produce normal alarm information and achieve the desired results. At the same time, the network behavior analysis method needs to be further improved in order to achieve better analysis results, and provide more reliable results for the detection system.

The article “Coherent Caesar Cipher for Resource Constrained Devices” says that cryptography is a cornerstone in the resource constrained networks and devices today. Many modern cryptosystems make it very difficult but not impossible for an attacker to determine the decoding key. Even though the key might be eventually determined by a skilled decoder, given enough time and effort, cryptosystems can still provides ample security to protect valuable information. Among various encryption techniques, Caesar cipher is one of the oldest technique to encrypt the valuable information. But it gets easily cracked due to its simplicity of operation. In this paper, a new algorithm is proposed i.e. Coherent Caesar Cipher (CCC), which is found to be more consistent and reliable as compared to other existing caesar cipher algorithms. Performance of CCC and conventional techniques are tested using various NIST suggested randomness evaluation tests along with brute force attack analysis.

The study “Research on Risk Propensity and Decision-making Satisfaction of Narcissistic Customer Investment Products based on Network Platform Questionnaire” explores the differences of narcissistic customer financial investment in the bank's risk propensity and decision-making satisfaction. Studies have shown that overt narcissism customers have the higher degree of risk propensity. Investment professionals in overt narcissism and risk propensity between positive regulation effect is obvious, and overt narcissism and the degree of satisfaction with decision making is related; covert narcissism customer and risk propensity and decision-making satisfaction relationship is not significant and investment professionals in covert narcissism and risk propensity among regulatory role is not obvious. Covert narcissism and overt narcissism tendency and differences in risk decision satisfaction provide new ideas for the design and marketing of financial products.

In the paper “A Chosen-Ciphertext Secure Fuzzy Identity-Based Proxy Re-Encryption Scheme”, Green and Ateniese introduced the notion of identity-based proxy re-encryption (IB-PRE), whereby the proxy can covert a ciphertext encrypted under the delegator's identity to an encryption under the delegatee's identity of the same message. In some situations, biometric, such as dactylogram, was used as identities. However, these biometric identities will inherently have some noise when they are sampled each time. To make identity-based proxy re-encryption flexible on identities, they introduced a new primitive called fuzzy identity-based proxy re-encryption (FIB-PRE), in which an identity is viewed as a set of descriptive attributes. In a fuzzy identity-based proxy re-encryption scheme, an identity W' can decrypt a ciphertext re-encrypted under another identity W, if

and only if W and W' are close to each other as measured by the "set overlap" distance metric. In this work, they first formulate the security model of a FIB-PRE scheme. Finally, they present a construction of FIB-PRE and prove its CCA security under the decisional bilinear Diffie-Hellman (DBDH) assumption in the random model.

May 2016

Jemal H. Abawajy, Deakin University, Australia
Bharat Bhargava, Department of Computer Science at Purdue, USA
Neal N. Xiong, School of Computer Science, Colorado Technical University, USA

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