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 "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET" proposes a DTSA(Detection Technique against a Sybil Attack) protocol so that it can provide vehicles with the secure information for the road situation and the traffic flow among vehicles and by detecting a Sybil attack. This DTSA uses SKC(Session Key based Certificate) to verify the IDs among vehicles, which generates a vehicle's anonymous ID, a session key, the expiration date and a local server's certificate for the detection of a Sybil attack. In conclusion, this DTSA reduces not only the detection time against a Sybil attack but also the verification time for ID by using a hash function and an XOR operation. Besides, a drivers' privacy can be protected by using an anonymous ID. This DTSA helps drivers drive safely with the reliable information of VANET and reduce traffic accidents.

Paper "Probability-based Tamper Detection Scheme for BTC-compressed Images Based on Quantization Levels Modification" proposed an image authentication scheme to protect the image integrity of the compressed images for block truncation coding (BTC).. In this scheme, the authentication data of each compressed image block is generated from the random value induced by the predefined random seed. The size of the authentication data can be selected according to the user's requirement. Then, the authentication data is embedded into the difference value between the quantization levels of each BTC-compressed image block.

In the paper "Multibiometrics Fusion for Identity Authentication: Dual Iris, Visible and Thermal Face Imagery", human identification via multibiometrics is a very promising approach to improve the overall system's accuracy and recognition performance. In recent years, several approaches toward studying the fusion strategies of different biometric evidence have been proposed. However, there are a number of major problems detected on some of those approaches such as weakness against spoofing attacks and higher acceptable error rate. In this paper, a novel multibiometrics fusion strategy based on dual iris, visible and thermal face traits is proposed. Initially, the features of related biometrics (dual iris, visible with thermal faces) are fused in feature level. Then, the matching scores of iris and face traits are fused via triangular norm. The proposed multibiometrics fusion achieves higher identification performance as well as immune to spoofing attacks.

The paper "Substitutive Mutual Authentication between Mobile Base Stations in Tactical Networks" proposes a cooperated mutual authentication scheme for mobile base stations

(MBS) that construct a Wireless Mesh Network (WMN) in the Tactical Information Communication Networks (TICN). To enhance the fighting capabilities and survivability of soldiers in battlefields, it is crucial to secure the communication and commands between soldiers and commanders. To achieve this goal, a reliable mutual authentication method is required to approve between MBS and the soldiers in the network. Authors apply EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) for mutual authentication between mobile base stations that each hold authentication servers. Also, they propose a cooperative authentication scheme that can substitute the authentication process between MBS and ultimately reduce the authentication overhead.

The Authors of "Secure Cryptographic Scheme based on Modified Reed Muller Codes" devised a new cryptosystem based on modified Reed Muller codes RM(r,m). The new cryptosystem is a modified version of Sidel'nikov's one. This allows to increase the security of the public key, and to reconsider Reed Muller codes as good candidates for using in secure encryption scheme. An efficient decoding with the Reed Muller decoding algorithm RM(r,m) and an increased level of security against attacks of the Sidel'nikov's crypto- system due to Minder and Shokrolahi are the main advantages of the modified version. Adding new columns implies longer codes, but this would not be a problem for decoding or deciphering because in decode one has only to deal with the words of the secret code belonging to the Reed Muller code RM(r,m). So the decoding phase would not suffer from this modification.

Paper "A Multimodal Fusion Algorithm Based on FRR and FAR Using SVM" presents remarkable improvements in recognition can be achieved through multibiometric fusion. Among various fusion techniques, score level fusion is the most frequently used in multibiometric system. In this paper, Authors propose a novel fusion algorithm based on False Reject Rate (FRR) and False Accept Rate (FAR) using Support Vector Machine (SVM). It transfers scores into corresponding FRRs and FARs, thus avoiding calculating posteriori probability of a certain score, as well as be capable of illustrating distribution of matching scores. The proposed method takes full advantages of both capabilities of FRR and FAR to describe the order of score and classification of SVM.

In the paper "Single Sign-On Scheme using XML for Multimedia Device Control in Children's Game Network based on OSGi service Platform", Authors proposes a single sign-on scheme in which a user offers his credential information to children's game network running the OSGi (Open Service Gateway Initiative) service platform, to obtain user authentication and control a remote device through a mobile device using this authentication scheme, based on SAML (Security Assertion Markup Language). By defining the single sign-on profile to overcome the handicap of the low computing and memory capability of the mobile device, Authors provide a clue to applying automated user authentication to control a remote device using a mobile device for distributed mobile environments including children's game network based on OSGi.

The paper "Toward Trust-based Privacy Protection in Consumer Communication" focus on trust based privacy protection in consumer communications by elaborating on three key issues: (1) quantification of privacy, (2) characterization of the relationship between privacy and trust, and (3) influence of trust on privacy protection. With trust based privacy protection, prior to an interaction, entities can set their privacy preferences conveniently and, during the interaction, they can choose their policies freely such as specifying whether privacy protection takes a higher priority than trust establishment, or vice versa.

The paper "Applying Basic-Elements and the Extension Theory to Alert-centric Event Correlation for Unified Network Security Management" introduces Extenics into the study on alert-centric event correlation for unified network security management and proposes a formalized approach using basic-elements based on the extension theory. The proposed approach utilizes the basic-elements to formalize the representations of alerts, events, and also correlation policies for network security in a unified manner, and then makes full use of the extension theory to formalize basic operators for extension expressions and extension functions in order to realize alert-centric event correlation. Validation scenarios of timing constraints show that, the proposed approach provides a prospective way to alert-centric event correlation for unified network security management by introducing basic-elements and utilizing extension expressions and extension functions with the use of containing analysis, sequencing analysis and extension transformations based on the extension theory.

The Authors of "Enhanced Security Communication System Using Digital Retrodirective Array Antenna" design a digital retrodirective array antenna (RDA) system possible for beamforming technology without any prior location information for signal quality improvement and security improvement. Fast beam tracking and beamforming technology are essential for the communication signal quality of high-capacity and high-quality.

Paper "Safety Properties based Scenario Generation for Model Checking Trampoline OS" deals with model checking that has proven to be a successful technology to verify real-time embedded and safety-critical systems. However an application of model checking in practice still requires manual construction of an environment model, which has a direct impact on verification cost. This paper suggests an automated scenario generation technique through a property-based static analysis of function-call relationship of the program source code. Authors present the scenario generation process and show application results on the Trampoline operating system using CBMC as a back-end model checker.

In the paper "The Firewall Rule Authentication Method Based on 6to4 Tunnel", the enterprise internal information security faced with many hidden trouble, and information leakage has been the largest security problem. Firewall is the main technology to solve information leakage, but end-to-end cryptograph tunnel communication can through firewall information filtering detection. In order to prevent the information leakage, it is common to add the block rules in firewall. There is short of a simple and effective verification method for the correctness of firewall blocking rules. Authors raise a method to verify firewall rules based on dual-protocol. With 64 tunnel technology, virtual an external node, analog communication scene between inside and outside, to verify the effectiveness of firewall rules.

Paper "An Improved Secure Dynamic ID-based Remote User Authentication Scheme with Key Agreement using Symmetric Cryptology" deals with a dynamic ID-based user authentication scheme that is designed to protect leakage of a user's partial information from intruders while enabling authenticated users to be granted access to the network service. In 2012, Wen and Li proposed a dynamic ID-based remote user authentication scheme with key agreement and claimed that their scheme resisted impersonation attacks and avoided leakage of partial information. However, Kim, *et al.*, described that Wen and Li's scheme could leak some key information to an adversary and is vulnerable to a man-in-the-middle attack launched by any adversary. This paper shows how to solve the vulnerabilities in Wen and Li's scheme.

In the paper "A Method of Threat Evaluation for Mobile Network", a cloud model was introduced to evaluate mobile network threat. As the qualitative knowledge representation and uncertainty handling method, the transform between qualitative concepts and their quantitative expressions become much easier and interchangeable. It bridges the gap between the rigidity of a mobile network system and the uncertainty of human thinking. Conclusion shows that the cloud model is effective and capable of directly analyzing the characteristics of mobile network threat evaluation.

The paper "A Watermarking for HTML Files Based on Multi-channel System" presented a novel HTML file watermarking method. An HTML file is to present the personality of a user or to advertise a company. In order to increase the robustness of the proposed watermarking, watermark data is concealed into the HTML file many times using a multi-channel system. The watermark data can be extracted from the watermarked HTML when arguing the copyright issue. Because the visual quality of watermarked HTML is one of the most important requirements in designing watermarking technique, the watermarked HTML will not have any perceptible distortion when watermark has been embedded into the HTML by the proposed method. Also, the voting strategy is adopted in the proposed method for achieving the robustness.

The Authors of "Wireless Structural Health Monitoring System Using ZigBee Network and FBG Sensor" develop wireless optical monitoring system using ZigBee network and Fiber Bragg Grating (FBG) sensor. FBG sensors are manufactured using the 248nm excimer laser and phase masks. The adopted wireless networking between PC and FBG interrogator is ZigBee, because ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on an IEEE 802 standard for personal area networks.

Paper "Hash-based RFID Mutual Authentication Protocol" states that with the development and application of RFID technology in Internet of Things (IOT), RFID system plays a more and more important role on privacy protection and information security of users. For the safety need of RFID system and the existing shortage of secure authentication protocols, Authors offer RFID mutual authentication protocol based on variable update. Mutual authentication is executed in RFID system through the characteristics of Hash function, which prevents the phenomenon of counterfeit in internal system. The method of periodic updates System initial value is adopted to improve the level of security authentication, which overcomes the various safety attacks. The protocol has certain advantages on security capabilities and algorithm complexity with high safety and practicality.

In the paper "Design and Implementation of a Network Attack Platform Based on Plug-in Technology", a large number of network security tools appear constantly in recent years. However, they all in the cohabitation of the state. This article designed a network attack platform based on plug-in technology, the prototype system has good interactivity and scalability. The system can guide the platform operator to complete a variety of different types and complete steps network attack experiments, help the platform operator research and learn network attack methods. Moreover, the Attack Knowledge Base can integrate new network attack methods. Attack Knowledge Base can be constantly updated, so that the platform can be applied to future network attack experiments. So the design of such a system has a high practical significance for teaching and researching network attack methods.

The paper “The Methodology of Security Management Cost Reduction using Security Level Lifecycle” focused on the two respects, one is security level lifecycle of the sensitive information (SI). The other is SI that has characteristics to decrease security level over time. Author proposed the method that total security management cost reducing than before applying by differential costing over security level lifecycle. Also, they considered of predictability on security level decrease together. The cost reduction target area through a comparison of the cost model is expressed.

In the paper “File Multi-analyses for Real-time Attack Source and Spread Site Trace”, says that recently, the illegal users with malicious intention utilize the file sharing site by making normal user's computer a zombie computer, which is a preliminary process for network intrusion attack. The propose scheme is divided into the method for real-time analysis for real-time tracking and the method of cooperative analysis method for non-real time analysis. By allowing the supervisors to choose the relevant analysis method selectively, a variable analysis depending on the network threat can be conducted.

Paper “FHGM: A Frequency Hopping Game Model with Communication Security Awareness for WSN” delas with wireless sensor networks (WSNs) that are in an open wireless environment which is complex and volatile, and often subject to inadvertent or intentional interference, sensor networks can use frequency hopping technology to get away from the interference. Therefore how accurate and timely frequency hopping is particularly important issue. To solve that, this paper built a Bayesian frequency hopping game model based on Nash equilibrium game theory. The formal definition and quantified description of the impact factors in the game model are described, and Bayesian Nash equilibrium is proved. Through the simulation and analysis shows that this model with communication security awareness can improve the accuracy of the frequency hopping, make the time of frequency hopping become more rational, prolong the network lifetime and maintain the overall network connectivity.

In the paper “Integrating Security Concerns into Software Development”, it has become clear in software development that functionality and security must go hand in hand in cases where security concerns are to be incorporated early in stages of design. An essential aspect of such a process is threat modeling that integrates security with functional specification. Such an approach includes construction of two models: a functional model and a security (threat) model. The problem of integration involves assimilating security concerns while developing system specifications. One solution is to represent the dynamic behavior of security attacks as statechart diagrams and integrate the attacks into the functional behavior of the system; however, such an approach results in a complex set of fragmented descriptions lacking an underlying conceptual representation that can be tailored to include security concerns. This paper introduces a flow-based diagrammatic representation that includes such features.

The paper “Towards Secure and Dynamic Password Based User Authentication Scheme in Hierarchical Wireless Sensor Networks” deals with two-factor user authentication which is an important research issue for providing security and privacy in hierarchical wireless sensor networks (HWSNs). In 2012, Das, Sharma, Chatterjee and Sing proposed a dynamic password-based user authentication scheme for HWSNs. This paper show weaknesses of Das, *et al.*'s scheme such as failing to prevent user clone and disclosing of base station's secret key.

A simple countermeasure to prevent proposed attacks is suggested while the merits of Das, *et al.*'s authentication scheme are left unchanged.

The Authors of "Can Friendship Be Counted on for Securing Wireless Ad Hoc Networks?" discusses that trust system plays a more and more important role in giving nodes incentives to cooperate in packet forwarding especially for wireless ad hoc networks. However, most existing works in this field either lack rigorous analysis of cost of their methods or have analysis in unrealistic models, which will clearly damage their effectiveness in real applications. In a previous work, Theodorakopoulos and Baras [1] develop a novel formulation of trust computation based on ordered semirings. In this paper, based on their work, Authors proposed FROST (FRiendship and Ordered Semirings based Trust system) for wireless ad hoc networks. FROST introduce notion of friendship to reduce the trust table size and overhead while building and maintaining the trust system in large scale networks. Moreover, FROST use a more effective decaying model to enable the trust system to be more adaptive to the changing environment.

Paper "An Improvement of Sood, *et al.*'s Authentication Scheme using Smart Card" presents that in 2004, Das, *et al.*'s proposed the dynamic ID-based remote user authentication scheme to protect the user's anonymity. However, in 2005, Chein, *et al.*'s and Liao, *et al.*'s demonstrated that Das, *et al.*'s scheme failed to protecting user's anonymity. In addition, they showed that it was susceptible to guessing attack, so that it might expose the password to the remote system. In 2006, Liou, *et al.*'s proposed a new scheme which aimed to resolve the security vulnerabilities of Das, *et al.*'s scheme such as mutual authentication and malicious server attacks. However, in 2010, Sood, *et al.*'s demonstrated that Liou, *et al.*'s scheme is susceptible to impersonal attack, malicious user attack, man in the middle attack and offline password guessing attack. To resolve those vulnerabilities, Sood, *et al.*'s proposed new scheme. However, as a result of analysis of the new scheme proposed by Sood, *et al.*, it is still vulnerable to malicious legal user attack and various attacks such as forgery, insider and database. In this paper, Authors propose an improvement to the Sood, *et al.*'s scheme in order to resolve such problems.

In the paper "Research On Efficient Turbo Frequency Domain Equalization In STBC-MIMO System", an efficient Turbo Frequency Domain Equalization (FDE) based on symbol-wise minimum mean-square error (MMSE) filtering is proposed for a novel space-time block code (STBC) MIMO system. The transmitter sends a separate data block via STBC using two antennas per group to get diversity gain. The receiver can effectively utilize inter-antenna interference (IAI) and inter-symbol interference (ISI) followed by frequency domain equalization to process soft interference cancellation (SIC). After frequency domain filtering, the symbol Log-likelihood ratio (LLRS) calculated from the outputs of equalizer is as the inputs of the soft-in soft-out (SISO) decoder.

The paper "An Innovative Two Factor Authentication Method: The QRLogin System" focuses on QRLogin, one of the leading two factor authentication programs, which successfully balances security with convenience. The system combines the traditional username and password with a time-sensitive, one time passcode. In contrast to this advanced security, users may conveniently login by scanning a code with their smartphone. Although the scanning feature of the QRLogin system is limited to smart phone owners, users may also login through the traditional ID and password method. The QRLogin system illustrates the

modern development of two factor authentication, which substantially increases the security of online transactions.

The paper "Analysis of Hash Functions and Cellular Automata Based Schemes" summarize hash functions and cellular automata based architectures, and discuss some pros and cons. Authors introduce the background knowledge of hash functions. The properties and theory of cellular automata are also presented with typical works. It is shown that cellular automata based schemes are very useful to design hash functions with a low hardware complexity because of its logical operation attributes and parallel properties.

The Authors of "A Robust Trust Management Scheme against the Malicious Nodes in Distributed P2P Network" aims to propose a robust trust management scheme to improve reliability and effectiveness of distributed P2P network by identifying these malicious threats and then limiting the attacker's participation. Especially, our scheme effectively manages for some attacks such as bad mouthing, on-off and sybil. The proposed scheme is expected to effectively protect attacks from malicious peers with improving credibility as well as exactness.

Paper "A Secure Real Media Contents Management Model Based on Archetypes using Cloud Computing" presents modifications and improvements to the interface of a secure real media contents management model with the intention of increasing security and usability. This paper examines a security technology that needs to be considered in the EHR (Electronic Health Record) service model. This EHR(Electronic Health Record) service model is suitable for example a secure real media contents management & processing. It constructs a model based on a MVC (Model-View-Controller) pattern based on access rights and distributed management. In particular, it constructs a test bed utilizing the Open EHR Tool which is a major topic in this area. Through this, it suggests the EHR service security control model in the context of the patient and medical team. The work aims for a new way of structuring, storing and managing patient data so that they can be shared and exchanged between different healthcare providers and other stakeholders in a safe and secure manner.

In the paper "Security Augmenting Scheme for Bus Information System based on Smart Phone", with the smart phone app, BIS can be implemented easily and conveniently without big cost. This BIS system, however, has a weak point that the location information of the bus can be revised easily. For the purpose of augmenting the security aspect of the proposed BIS service, this paper introduces the security augmenting scheme for the bus information system that is composed of the smart phone app without extra infrastructure like wireless LAN or wireless relay system.

Paper "Security in Graphical Authentication" deals with Graphical Authentication Systems that are a potential replacement or supplement for conventional authentication systems. Several studies have suggested graphical authentication may offer greater resistance to guessing and capture attacks but there are other attacks against graphical authentication including social engineering, brute force attacks, shoulder surfing, intercepted communication and spyware. This paper gives a brief description and classification of different graphical password schemes followed by information about vulnerabilities in the various schemes and recommendations for future development.

In the paper "Eliminate Evading Analysis Tricks in Malware using Dynamic Slicing", Author proposes an approach to deal with anti-emulation using instruction traces and dynamic slicing. With a difference from trace matching solutions presented in existing references, the approach is performed on one instruction trace derived from our dynamic analysis platform.

The paper "Robust Video Watermarking Based on Temporal Modulation with Error Correcting Code" presented a novel robust video watermarking algorithm that satisfies robustness and real-time performance requirements in client-side embedding environments such as IP TV set-top boxes. A watermarked video is generated by temporally modulating the mean chrominance value of each chrominance channel in relation to the watermark pattern according to the watermark message. The watermark pattern is generated based on a histogram analysis of the luminance channel. To improve the robustness, Authors employed the BCH codes followed by repetition codes during the encoding of the watermark message.

The Authors of "Random Selection of Multiple Spreading Codes Enhances the Security of DSSS Transmission (RSMC-DSSS)" focus on Spread Spectrum technique that transmits the information message (signal) over a bandwidth much larger than its frequency contents or the original bandwidth of information message. In SS technique, a signal (having a specific bandwidth) is spread in the frequency domain and results in a signal having wider bandwidth. Remember, the new resulting bandwidth of a signal is much larger than the minimum required frequency spectrum. In Direct Sequence Spread Spectrum, *i.e.*, DSSS (one of the common techniques of SS) the transmitting information signal is multiplied or combined with the spreading signal (usually Barker code) of wider bandwidth and results in a modulation signal that take up the wide bandwidth of the spreading signal. This new consequential signal is then combined with a carrier signal before transmission. The most important advantage of DSSS technology is the accepted transmission security. In this paper, a novel scheme is proposed that helps out the traditional DSSS system to enhance the transmission security by using random selection of multiple spreading codes in DSSS. In this paper the 11-bit spreading (Barker's) code is taken under the consideration as the spreading code.

Paper "Page Mapping Scheme to Support Secure File Deletion for NAND-based Block Devices" presents a method for secure file deletion in NAND-based block devices. The presented scheme maintains the over-write count and the physical locations of the original data. If the over-write count exceeds a predefined threshold, the scheme finds the original data that has been invalidated by previous over-write operations and removes the original data using the block erasure operation. The erased data is irrecoverable.

The paper "Text Clustering using Semantic Features for Utilizing NFC Access Information" proposes a text clustering method using the reweighted term based on semantic features for utilizing NFC content. The proposed method uses text document samples of cluster by user to reduce the semantic gap between the user's requirement and clustering results by machine for utilizing NFC access information. The method can enhance the text clustering because it uses the reweighted term which can well represent an inherent structure of text document set relevant to a user's requirement regarding NFC tags.

In the paper "A Comparative Study on Tangerine Detection, Counting and Yield Estimation Algorithm" a new counting algorithm for tangerine yield estimation is adapted to obtain better results with respect to partially/semi partially occluded tangerine and its clusters. To optimize tangerine counting, and to minimize typical background noises from orchards

(*i.e.*, bare soil, weeds, and man-made objects), a tangerine fruit counting algorithm is implemented, and compared between before harvesting, after harvesting tangerine fruits, and results of yield estimation through tangerine flower recognition. Under natural lighting conditions prediction of the tangerine fruits from the orchards is computed and compared based on observers, and with tangerine counting algorithm.

In the paper "Fault Localization Method of Software Defects based on Dependencies Analysis of Program Structure", Software defects are the major risks of system stable operation. Its error localization technology of automation is one of the key research content for trust computing and software assurance. This paper has proposed a new model, which integrates the current methods by analyzing the program structure. Authors put forward a new automated fault localization method, this method without the degree loss of automation, at the same time, particle size down to basic positioning code statements, makes the position more accurately.

May, 2013

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

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