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 15 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 Novel Relational Database Watermarking Algorithm Based on Clustering and Polar Angle Expansion" proposes a novel relational database watermarking scheme based on a fast and stable clustering method on database tuples, which adopts Mahalanobis distance as the similarity measurement. Before the process of watermark embedding and detecting, the databases tuples are adaptively clustered into groups according to the length of binary watermark. Moreover the watermark segments are respectively embedded into or detected from those groups according to the numeric field's Lowest Significant Bit (LSB) and polar angle expansion. The majority decision strategy is used to determine the value of watermark bit in blind detection process.

Paper "TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing" discusses the countless advantages of cloud computing that has brought a massive change to the lifestyle and the way to cope with the world today, yet the cloud has to reach maturity. However, the main barrier to its widespread adoption is the security and privacy issues. In order to create and maintain mutual trust among the customers and the cloud service providers, a well – defined trust foundation should be implemented. The data stored in the cloud remotely by individual customer or an organization, so they lost control over the data, thus creating a security dilemma. The most challenging and hot research area in cloud computing now a day is the data security and access control. An effective measure to protect cloud computing resources and services in the start is to implement an access control mechanism. In this paper the features of various access control mechanisms are discussed and a novel framework of access control is proposed for cloud computing, which provides a multi - step and multifactor authentication of a user. The model proposed is well-organized and provably secure solution of access control for externally hosted applications.

In the paper "E-LPG: Energy Efficient Location Privacy Scheme against Global Attackers in Sensor Networks", many sensor network security schemes protect the content of messages, while the contextual information is left vulnerable by disclosing the location of the monitored objects. Preserving location privacy is important and one of the most challenging issues in many mission critical sensor network applications. Prior solutions are mostly designed to protect privacy from local attackers who eavesdrop on traffic in a small region at a time. However, they can be easily defeated by highly motivated global attackers that can trace the entire network's communication events. Although a few recent privacy solutions are proposed against global attackers, they suffer from significant communication overhead as they inject dummy traffic or send messages in a globally synchronized manner. As a result, they

consume a lot of energy to maintain a desired privacy level that makes the network lifetime shorter. An energy-efficient source location privacy preserving solution, named the Energy Efficient Location Privacy Scheme against global attackers (E-LPG) is proposed. E-LPG hides original source locations through a spatial scatter of messages using stealthy wormholes and through a temporal scatter using random delays when permitted. With a limited number of wormholes, E-LPG can achieve a high privacy level without incurring extra communication overhead.

The paper "Cryptanalysis of Server-Aided Password-Based Authenticated Key Exchange Protocols" identified an inherent flaw in the design of Nam, *et al.*'s three-party PAKE protocol (IEEE Communications Letters, 13(3), 2009) and Lu and Cao's protocol (Computers & Security, 26(1), 2007) and demonstrated that both protocols are susceptible to a previously unpublished off-line dictionary attack. By identifying this design flaw, similar structural mistakes can be avoided in future design.

The Authors of "An Empirical Study of Metric-Based Methods to Detect Obfuscated Code" present an empirical evaluation of three text-based metrics to identify obfuscated code. Our experiment shows that the effectiveness of these metrics depends on the obfuscators: there are cases in which the metrics allow the proliferation of false positives (*i.e.*, misclassification of clear code as obfuscated code), which is bothering but not dangerous, and cases where false negatives (*i.e.*, misclassification of obfuscated as clear code) proliferate, which is definitely more dangerous.

Paper "A Faster Cryptanalytic Time-Memory Tradeoff" presents that there has been extensive research on a cryptanalytic time-memory tradeoff for recent 30 years. Since Hellman's work in 1980, some improved variants and techniques have been proposed, and the rainbow method is known as the best time-memory tradeoff. As for the memory size, however, the required number of bits per start point and end point was not explicitly considered in these works. With this, a new time-memory tradeoff is proposed and analyzed the expected cryptanalysis time.

In the paper "X-Policy: Knowledge-based Verification Tool for Dynamic Access Control Policies", Authors discuss about verifying the correctness of large, complex and dynamic access control policies by hand is insufficient and error-prone. They present X-policy, a knowledge-based verification tool that can analyse the system's vulnerabilities where the attackers can act as a coalition of users, use the system, share knowledge and collaborate with each other to achieve the attack. A policy language is presented that is able to express dynamic access control policies and a corresponding query language. They model the EasyChair conference management system and analyse in details three security properties of EasyChair using our model.

The paper "Study on A Secure Remote User Authentication Scheme Using Smart Cards" presents a discussion about a remote user authentication scheme that is a kind of way to authenticate the communication parties who transmit messages through an insecure channel. Researchers in this area have proposed some approaches during the last couple of decades. Unfortunately, most of them are proved to be insecure against various attacks. In 2009, Kim and Chung improved Yoon and Yoo's scheme, and claimed that their scheme can prevent masquerading attack as well as resist to other malicious attacks. However, it is being found that Kim and Chung's scheme is still not secure enough, especially in preventing off-line

password guessing attack. In this study, a more secure and practical remote user authentication scheme is proposed to resolve all of the aforementioned security vulnerabilities while preserving the merits of Kim-Chung's scheme.

The paper "Classification of Symmetric Key Management Schemes for Wireless Sensor Networks" defines WSN as the collection of thousands of tiny sensor nodes, which have the capability of sensing, computing and transmitting the information in the network. Due to the low circuit design, it has some resource constraints but efficient to carry the information through wireless communication. But the exchange of information in a secure manner is critical in WSN. There are many techniques developed in recent years for the security purposes, one of the area is the key management. Key management is the challenging issue in sensor networks. The key management techniques for wireless sensor networks and classification have been presented based on the encryption techniques.

The Authors of "On the Security of H^2-MAC" propose an efficient method to break H^2-MAC, by using a generalized birthday attack to recover the equivalent key, under the assumption that the underlying hash function is secure (collision resistance). The equivalent key of H2-MAC is successfully recovered instantiated with any Merkle-Damgård hash function in about $2^{n/2}$ on-line message authentication code (MAC) queries and $2^{n/2}$ off-line MAC computations with good probability. The pseudo random function-affix (PRF-AX) assumption of the origin security proof of H^2-MAC is argued, and proved that the security of H^2-MAC is dependent on the collision resistance of the underlying hash function, instead of the PRF assumption.

Paper "A New NUI Method for Hand Tracking and Gesture recognition Based on User Experience" explains a study on natural user interface (NUI) in human gesture recognition using RGB color information and depth information by Kinect camera from Microsoft Corporation. To achieve the goal, hand tracking and gesture recognition have no major dependencies of the work environment, lighting or users' skin color, libraries of particular use for natural interaction and Kinect device, which serves to provide RGB images of the environment and the depth map of the scene were used. An improved CamShift tracking algorithm combined with depth information is used to tracking hand motion, and then an associative method of HMM and FNN is propose for gesture recognition step.

In the paper "Efficient and Non-Interactive Hierarchical Key Agreement in WSNs", it is discussed that wireless sensor networks (WSNs) have many applications, vary in size, and are deployed in a wide variety of areas. They are often deployed in potentially adverse or even hostile environment so that there are concerns on security issues in these WSNs. Sensor nodes used are resource-constrained, which make security applications a challenging problem. Key agreement is a fundamental security service in WSNs; it enables sensor nodes to communicate securely with each other using cryptographic techniques. However, due to the resource constraints on sensor nodes, it is infeasible to use traditional key management techniques such as public key cryptography and key distribution center. Recently, Guo, *et al.*, proposed an efficient and non-interactive hierarchical key agreement protocol applicable to mobile ad-hoc networks, which has good properties including non-interactive, hierarchical, resilient, etc. The purpose of this paper is to propose a non-interactive hierarchical key agreement protocol over the hierarchical WSNs, which is a revision of Guo, *et al.*'s protocol for the WSNs due to their protocol's good properties.

Paper "An Empirical Analysis on Development Effects of Diabetic Prevention Information System" deals with an empirical analysis on development effects of diabetic prevention information system. The subjects of this study were 114 patients who had been visited a general hospital which located in urban area. The validity of the developed information system was estimated using intervention method that measured action-oriented, relevant, and effect of time elapsed between groups.

In the paper "Cryptography: A New Approach of Classical Hill Cipher", Author proposed a robust Hill algorithm (Hill++). The algorithm is an extension of the Affine Hill cipher. A random matrix key is introduced as an extra key for encryption. Moreover, an involuntary matrix key formulation is also implemented in the proposed algorithm. This formulation can produce an involuntary key where a same key can be used for both encryption and decryption. Testing on the proposed algorithm is carried out via two approaches, that is through comparative study and statistical analysis. Comparative study shows that Hill++ is resistant to all zeroes plaintext block encryption and does not face the non invertible key matrix problem as what was faced by the original Hill, AdvHill and HillMRIV algorithms. Apart from this, the encryption quality of the proposed algorithm is also measured by using the maximum deviation and correlation coefficient factors.

The paper "Face Recognition via Local Directional Pattern" proposed an illumination-robust face recognition system via local directional pattern images. Usually, local pattern descriptors including local binary pattern and local directional pattern have been used in the field of the face recognition and facial expression recognition, since local pattern descriptors have important properties to be robust against the illumination changes and computational simplicity. Thus, this paper represents the face recognition approach that employs the local directional pattern descriptor and two-dimensional principal analysis algorithms to achieve enhanced recognition accuracy. In particular, a novel methodology is proposed that utilizes the transformed image obtained from local directional pattern descriptor as the direct input image of two-dimensional principal analysis algorithms, unlike that most of previous works employed the local pattern descriptors to acquire the histogram features.

March, 2013

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

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