This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30051801

Reproduced with the kind permission of the copyright owner.

Copyright : 2012, SERSC
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 21 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 “Multi-Layer Data Encryption Using Residue Number System in DNA Sequence”, merge the usages of DNA sequences and Residue number system in encryption systems. The message which is coded will be secretly impeded inside the DNA sequence. This merge will be leaded to perform multilayer encryption with different keys - that can be used as a hash function - versatile alternatively to increase the security and more flexibility, with less complexity.

Paper “A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography” presents a technique for secret communication using cryptography and steganography. The cryptographic algorithm is a block cipher with a block length of 128 bits and key length of 256 bits. The secret message is encrypted by this block cipher. Two cipher text bits are to be embedded in each pixel of the image. As the embedding locations are decided at the run time of the algorithm, so it is called as dynamic steganography.

The paper “Security Threats in Cloud Computing Environments”, provide security topic in terms of cloud computing based on analysis of Cloud Security threats and Technical Components of Cloud Computing. Based on these Cloud Security threats, the following items are main topic for Cloud Security standardization: Security Architecture/Model and Framework; Security Management and Audit Technology; Business Continuity Planning (BCP) and Disaster Recovery; Storage Security; Data and Privacy Protection; Account/Identity Management; Network Monitoring and Incident Response; Network Security Management; Interoperability and Portability Security; Virtualization Security; and Obligatory Predicates.

The paper “Analysis of Operator Errors in Routing Policy Configurations”, focuses on the routing policy configurations, that are one of the crucial element of network configurations since they deal with a network’s connectivity, quality of service, and security. The languages and user interfaces used to configure routing policies are not well suited to network operators’ needs which often lead to configuration errors and lengthen the time taken to resolve problems. Authors observe that current routing policy configuration management have four major problems, including both technical and usability problems: (i) the large number of obsolete and irrelevant configurations, (ii) subtle interactions with multiple relevant technologies, (iii) the overlapping, complex set of configuration options, and (iv) insufficient
support for the efficient reuse of common configuration segments. Based on this observation, a set of guidelines for creating more usable configuration management was proposed.

The Authors of “Bank Web Sites Phishing Detection and Notification System Based on Semantic Web technologies” propose a system for client-side defenses such as browser plugins and classification techniques that are adopted in phishing detection scenarios. The system inspects the HTML pages as an annotated document represented or embedded in XHTML format using RDF annotations. The results show a promising findings in the area of phishing detection that requires hand-in-hand collaboration between various banking branches and the country’s central or authorized bank. Additionally, the system notifies the corresponding bank about the phishing web sites, and the bank in turn notifies its clients.

Paper “Enhancing Grid Security using Quantum Key Distribution” presents a model for the exploitation of QKD security networks in high performance distributed computing applications, such as grid computing. Quantum Key Distribution (QKD) is a secure key distribution technology, which provides information theoretic or unconditional security. BBN DARPA quantum network and SECOQC network of secrets are the examples of such networks. Research is also in progress for the integration of QKD with the protocols in different layers of OSI model. Integration of QKD in point-to-point protocol (PPP) OSI layer 2 and with IPSEC at OSI layer-3 is the examples of such research efforts. All these steps are leading towards the utilization of QKD technology for enhancing the security of modern computing applications on the Internet.

In the paper “Integration of Sound Signature Authentication System”, Authors proposed a sound signature graphical password consists of user-chosen click points in a displayed image. In order to store passwords in cryptographically hashed form, small uncertainties in the click points from having any effect on the password needs to be prevented and this is achieve by introducing a robust discrimination, based on multigrid discrimination.

The paper “An Anti-Shoulder Surfing Mechanism and its Memorability Test” proposed an anti-shoulder surfing mechanism called Painting Album Mechanism to improve security of mobile device graphical password towards shoulder surfing attack. This mechanism is constructed based on concept of painting album, and it is consists of three input schemes called Swipe Scheme, Color Scheme, and Scot Scheme. In this paper, usability of this mechanism have been verifying with the memorability test. 30 respondents were authenticating with these three input schemes with multiple authentications. Results were showing Painting Album Mechanism is usable since respondents were succeeding in recalling theirs passwords in acceptable period of time.

The paper “Modeling the Forensics Process”, proposes an abstract model of the digital forensic model based on a new flow-based specification methodology. It is shown in examples that the method can uniformly specify the forensic process in various phases and across roles. It also provides more exact description where “things” (e.g., information, evidence) are separated into different streams of flow. Most forensic models focus on the investigative process and its different phases and are characterized by a rather informal and intuitive approach.

The Authors of “Web Service Selection Using Quality Criteria and Trust Based Routing Protocol” introduces a new algorithm for effective construction of the primitive services
according to their quality criteria. A trust based ranking algorithm is employed to diminish the service with lower qualities. Web Services are applications that perform desired tasks. Such as basic network connectivity to sophisticated compound tasks. Service Composition is the construction of complex services to enable different tasks. Therefore, enabling a rapid and effective composite of services is crucial point in efficiency of composite web services.

Paper “Design and Analysis of a Non-deterministic Digital Signature Protocol” describes a modular arithmetic-based signing scheme called NDSP which combines essentially optimal efficiency with attractive security properties. Signing takes one RSA decryption plus some hashing, verification takes one RSA encryption plus some hashing, and the size of the signature is the size of the modulus. Assuming the underlying hash functions are ideal, our schemes are not only provably secure, but are so in a tight way — an ability to forge signatures with a certain amount of computational resources implies the ability to invert RSA (on the same size modulus) with about the same computational effort.

The paper “The Risks Facing China’s Mining Companies – An Analysis from Global Perspective”, works through various risk scenarios and performs impact analysis, and then gives suggestions about risk management and control from both macro and micro perspectives. Mining operations represent an economic activity with plenty of decision problems involving risk and uncertainty. While underlying risks do not vary significantly from year to year, their level of acuteness and priority can change depending on the economic environment. With the development of economic globalization, China’s mining companies are exposed to a higher than average level of risks, especially risks from political and economic policies of the host country, as well as financials.

Paper “An Improved Secure Anonymous Protocol for Distributed Computer Networks” adopt Elliptic Curve Cryptography (ECC) to reduce the computational cost in Cui and Cao’s protocol, and propose an indexing trick to speed up searches of legitimate users. The proposed scheme maintains the characteristic of obfuscating user identity to thwart identification attempts. Cui and Cao’s protocol is a secure anonymous key agreement for distributed networks, in which users collect other identities to utilize in communication so attackers cannot determine the real identity of the user (2010). However, this protocol suffers the drawback of high calculation requirements.

In the paper “Improvement of Convertible Authenticated Encryption Schemes and Its Multiple Recipients Version”, Authors separately points out that any adversary can forge a converted signature in Araki's scheme and Ma-Chen's scheme. Moreover, they further improve the weakness in Wu-Hsu's scheme, which is to convert the signature into an ordinary one should divulge the message. The improved scheme not only solves the weakness but also reduces the computational complexities in both sides of signer and recipient. Furthermore, the proposed convertible authenticated encryption scheme is extended for multiple recipients. The message can be recovered and verified by a group with multiple recipients.

The paper “A Stronger Formal Security Model of Three-party Authentication and Key Distribution Protocol for 802.11i” analyzes the existing formal security models of three-party authentication and key distribution protocol for 802.11i, which are extended BR and Extended CK models. Authors propose the flaw about the definition of session identifier in Extended CK model and present the limitation of matching conversation defined in Extended BR model. In order to fix these problems and provide a perfect model for provable security
protocol, a new stronger formal security model of three-party authentication and key distribution protocol is defined by “efficient AP” according to the rules of 802.11i standard, and they present a new provable secure EAP-TLS protocol in our model. The new formal security model proposes a better method to design provable security three-party authentication and key distribution protocol in WLAN. In addition, this paper also suggests an idea to define the authentication relationships in special application environment.

The Authors of “Modeling of Document Security Checkpoint for Preventing Leakage of Military Information” designed a document security checkpoint for inspecting leakage of sensitive documents including military information from the internal to the outside network. The designed model checks all documents when they are downloaded, sent, and printed. The model consists of four modules: authentication module, access control module, misuse monitor module, and tracking module. The authentication module checks the insider’s information and after which allows an insider to log on to the system. The access control module authorizes an insider to do operations (read, write) according to his role and security level. The pattern monitor module watches an insider’s abnormal access on documents as comparing the insider’s actual process to current process profile in database. The tracking module traces documents sent outside and verifies fabrication of documents. The document security checkpoint prevents indiscriminate access to documents and it does not allow access to documents unrelated to the insider’s duty and security level. Even though the document is illegally leaked by an insider, it can be tracked by watermarking techniques in tracking module.

Paper “Homomorphic Encryption to Preserve Location Privacy” considers a group of users who wants to use a location-based service while preserving their location privacy. A solution for this scenario is proposed and compares it with the previous solution. Analysis of The protocol shows the effectiveness of the proposed approach in terms of computation and communication costs.

In the paper “Compliance Risk Assessment Measures of Financial Information Security using System Dynamics” Authors analyze relationships between EFT (Electronic Financial Transaction) Act of Korea and risk assessment standards and propose the map that helps financial institutions determine the priority of security control areas. It is a new method for financial information security risk identification and assessment through correlation analysis between the variety security standards and requirements. They attempt to integrate different information security standards and propose risk assessment measures specializing in financial companies based on the mixed methods of quantitative and qualitative methods to determine the priority through the calculation of weights.

The paper “Design and Implementation of a Compiler with Secure Coding Rules for Secure Mobile Applications” define the secure coding rules that reflect the characteristics of the mobile environments and applications by the analysis of the existing secure coding rules. The compiler to inspect vulnerabilities of the mobile applications using defined secure coding rules in the coding stage will be designed and implemented.

The paper “Security Analysis of the Masking-Shuffling based Side Channel Attack Countermeasures” suggest a new practical method called a Biasing Power Analysis (BPA) to find a secret key used in an AES based on a masking-shuffling method without the use of the time position and template information of the masking value. Authors conducted an
experiment on a BPA attack against a 128-bit AES secret key based on a masking-shuffling
method operating on an MSP430 chip and succeeded in finding the entire secret key. The
results of this study can be utilized for next-generation ID cards to verify their physical safety.

The Authors of “Design of User Information Profiling for Consolidated Authentication in
N-Screen Environment” presents the user profile design method for the integrated
authentication within the service based on HTML5. Authors intend to discuss the measure
which enables the integrated management of personal information within the heterogeneous
devices using the designed integrated user profile information and can help provide the
authentication by phase depending on the selection of user.

October, 2012

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

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