Editorial

Chan Yeob Yeun* and
Mohamed Jamal Zemerly

Computer Engineering Department,
Khalifa University for Science, Technology and Research,
Sharjah Campus, P.O. Box 573 Sharjah, UAE
E-mail: cyeun@kustar.ac.ae
E-mail: jamal@kustar.ac.ae
*Corresponding author

Galyna Akmayeva

Infonomics Society,
1 The Greensted, Essex, Basildon, SS14, UK
E-mail: g.akmayeva@infonomics-society.org

Biographical notes: Chan Yeob Yeun received his MSc and PhD in Information Security from Royal Holloway, University of London, respectively. After his PhD, he joined Toshiba TRL in Bristol, UK. Then, he became the Vice President at LG Electronics, Mobile Handset R&D Center in 2005. He was responsible for developing niche and World Class Convergence Technologies that include World First 3G and Mobile TV such as DVB-H, TDMB, MediaFLO and 3G and Mobile TV with Mobile Security such as CAS and DRM. He left LG Electronics in 2007. Then, he joined at KAIST-ICC until August 2008 and moved on to Khalifa University of Science, Technology and Research (KUSTAR). He currently enjoys lecturing MSc in Information Security at KUSTAR. He published various international conferences and journals. He has been a regular invited speaker at ITU Telecom World, 3GSM World Congress and various international conferences.

Mohamed Jamal Zemerly received his MSc from University College Cardiff, Wales and his PhD from The University of Birmingham, UK. He has published many research papers. He was an organising committee member of many conferences ICSPC 2007, RISC 2009. He is currently the Chair of the Computer Engineering Department in Khalifa University of Science, Technology and Research (KUSTAR). He has a great experience in research projects.

Galyna Akmayeva is a Consultant in e-learning security enhancement. Her research interests are in the fields of e-learning security. She has authored and co-authored many papers in e-learning security and trust related field. She has organised and chaired number of international conferences and workshops and a Guest Editor to *IJITST*.

Copyright © 2010 Inderscience Enterprises Ltd.

This special issue 'Radio frequency identification applications and networks security' of *IJITST* includes some research papers that present the best selected papers of ICITST 2009, which was held in London. The papers have been extended and updated to fulfil *IJITST* standards. The summary of the papers in this special issue are as follows.

The 'Lightweight mutual authentication protocol for securing RFID applications' by Mouza Ahmad Bani Shemaili, Chan Yeob Yeun and Mohamed Jamal Zemerly, addresses security, privacy and authentication and proposes a lightweight mutual authentication suitable to be implemented for the passive RFID tags. The proposed protocol is simple, low cost and low power consumption as well as requires low computation as it uses a light shrinking generator that could be considered an alternative for the use of the well known one time pad algorithm.

The 'A survey on RFID security and provably secure grouping-proof protocols' paper by Dang Nguyen Duc, Divyan M. Konidala, Hyunrok Lee and Kwangjo Kim, present the first security definition for a secure grouping-proof protocol for RFID tags. The definition is then used to analyse the security of our proposed grouping-proof protocol which employs a (n, n)-secret sharing scheme to solve the scalability problem of previous protocols. In the first part of this paper, the authors attempt to summarise current research in the field of RFID security and discuss some of their open issues. While the second part of the addresses some of the open problems we suggested in the first part. In particular, we deal with scalability problem of existing grouping-proof protocols for RFID tags.

Ahmad R. Amran, Raphael C-W. Phan, David J. Parish and John N. Whitley, paper titled the 'Evidential structures and metrics for network forensics' takes a step forward showing how security metrics can be used to sustain a sense of credibility to network evidence gathered as an elaboration and extension to an embedded feature of network forensic readiness (NFR) – redress that is defined as holding intruders responsible. With less resource intensive and minimum costs, appropriate civil and criminal procedures can then ensue, based on the severity of the malicious activity and associated damage. The evidence gathered through the measurement and metrics shall become part of the active defence in which adversary will be aware that such organisation has the ability to catch and prosecute and thus, dissuade them from conducting malicious activities and attacks. The forensic metrics system can be viewed as independent from the need for specific technology-dependent tools. Its main purpose is also demonstrated in sustaining a sense of credibility as to the evidence gathered.

One approach to authorisation of mobile agents is to use XACML policies by assigning roles to agents and then enforcing role-based authorisation. The paper by Awais Shibli, Alessandro Giambruno, and Sead Muftic, 'Security architecture and methodology for authorisation of mobile agents' show how traditional XACML polices, used for user access control in distributed environments, can be used for mobile agents' access control. The authors use XACML polices to manage delegation of access rights from users to agents, while at the same time following the core principles of the XACML standard. This paper proposes combination of policies that map users to their mobile agents and make access control decisions for mobile agents by evaluating complex policy sets. We have identified all architectural components along with the operations required for enforcement of authorisations of mobile agents during execution.

Ali Sydney, Caterina Scoglio, Mina Kamel, and Phillip Schumm, paper titled the 'Characterising the robustness of complex networks' investigates the characteristics of network topologies that maintain a high level of throughput in spite of multiple attacks. To this end, we select network topologies belonging to the main network models and

some real world networks. The authors consider three types of attacks: removal of random nodes, high degree nodes, and high betweenness nodes and use elasticity as our robustness measure and, through our analysis, illustrate that different topologies can have different degrees of robustness. In particular, elasticity can fall as low as 0.8% of the upper bound based on the attack employed.

In 'CryptoNET: a model of generic security provider' paper by Abdul Ghafoor Abbasi, Sead Muftic and Gernot Schmölzer, reflects the security requirements derived from a wide range of applications; from small desktop applications to large distributed enterprise environments. Based on the abstract model, this paper describes design and implementation of an instance of the provider comprising various generic security modules: symmetric key cryptography, asymmetric key cryptography, hashing, encapsulation, certificates management, creation and verification of signatures, and various network security protocols. This paper also describes the properties extensibility, flexibility, abstraction, and compatibility of the Java security provider. The extension of this work is mSecurityProvider (mini security provider) which can be designed as an applet for smart cards, lightweight devices and mobile agents (part of baggage during travelling).

The 'On the security issues of NFC enabled mobile phones' by Lishoy Francis, Gerhard Hancke, Keith Mayes and Konstantinos Markantonakis, investigate the possibility that a near field communication (NFC) enabled mobile phone, with an embedded secure element (SE), could be used as a mobile token cloning and skimming platform. The authors show how an attacker could use a NFC mobile phone as such an attack platform by exploiting the existing security controls of the embedded SE and the available contactless APIs. To illustrate the feasibility of these actions we also show how to practically skim and emulate certain tokens typically used in payment and access control applications with a NFC mobile phone. In conclusion, the findings indicate that the embedded SE with the existing security controls and the available contactless APIs could be exploited to configure the mobile phone as a contactless attack platform. These issues needs to be urgently addressed with effective security countermeasures in place.

Daniel Caragata, Safwan El Assad, Hassan Noura and Ion Tutanescu, paper titled the 'Secure unicast and multicast over satellite DVB using chaotic generators' proposes a security upgrade for IP communications over satellite DVB that is suited for the characteristics of satellite communications and that offers support for both unicast and multicast communications. The usage of chaotic functions is proposed both for the generation of new keys and for the encryption of data. The authors propose the use of a strong chaotic key generator and of a robust encryption algorithm, which have been previously studied, to enhance the properties of the system.

In 'Framework for secure wireless health monitoring and remote access system', by Mahmoud Al-Qutayri, Chan Yeob Yeun, and Khalifa Belghuzooz, presents the design and implementation of a prototype secure system to monitor patients in hospitals. The system also enables remote access to the patient database by the appropriate health professional. This system integrates various wireless technologies in a secure framework. The system enables the supervising health professional to set various health parameters to be monitored. The prototype system consists of three modules: the sensing side where it captures reading from sensors and sends them to the second module which is the server. The server sends SMS notification to the supervising doctor in case of abnormal readings. The system provides many services: data management for patient and doctors through

graphical user interface, SMS notifications in case of critical condition, patient monitoring by capturing readings from sensor side, sensor side configuration and patient data enquiry using a mobile handset.

Acknowledgements

The guest editors would like to thank the Editor-in-Chief of *IJITST*, Professor Dr. Charles A. Shoniregun, and all the authors who submitted papers to this special issue. Also, we would like to show appreciation to all the authors of the selected papers published in this issue, for their enthusiasm, and commitment.