Preface

Al-Sakib Khan Pathan*

Department of Computer Science,
Kulliyyah (Faculty) of Information and Communication Technology,
International Islamic University Malaysia (IIUM),
Jalan Gombak, 53100, Kuala Lumpur, Malaysia
E-mail: sakib.pathan@gmail.com
*Corresponding author

Muhammad Mostafa Monowar

Department of Information Technology,
Faculty of Computing and Information Technology,
King AbdulAziz University,
Jeddah-21589, P.O. Box: 80221, Kingdom of Saudi Arabia
E-mail: hemal.cu@gmail.com
E-mail: monowar@ieee.org

Biographical notes: Al-Sakib Khan Pathan received his PhD in Computer Engineering in 2009 from Kyung Hee University, South Korea. He received his BSc in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh in 2003. He is currently an Assistant Professor at the Computer Science Department in International Islamic University Malaysia (IIUM), Malaysia. He holds editorial positions in various top-ranked journals and is editor/author of six books. He also holds various chairing and committee membership positions in numerous international conferences, as well as serving as a referee of some renowned journals. He is a member of IEEE (USA), IEEE ComSoc (USA), IEEE ComSoc Bangladesh Chapter, and several other international organisations.

Muhammad Mostafa Monowar is currently working as an Assistant Professor at the Department of Information Technology in King AbdulAziz University, Kingdom of Saudi Arabia. He is also an Associate Professor (on leave) at the Department of CSE, University of Chittagong, Bangladesh. He received his PhD in Computer Engineering in 2011 from Kyung Hee University, South Korea. He received his BSc in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh in 2003. He has served as a programme committee member in several international conferences/workshops. He is currently serving as an Associate Editor of IJIDCS, and as guest editor of some special issues of *IJCSE*.

A massive proliferation of web applications has been observed in recent years as the web is embraced by millions of businesses and government sectors as an inexpensive channel to communicate and exchange information with prospects and transactions with customers. Web applications are usually used from a web browser and, along with the typical informative site-surfing, they cover a range of activities such as e-banking, webmail, online shopping, community websites, blogs, vlogs, network monitoring and bulletin boards, while the internet is the implemented networking infrastructure that connects millions of computers together in different geographic locations.

Web applications indeed have become a ubiquitous phenomenon and central part of our everyday cyber life; however, these applications do raise a number of security concerns. Serious weaknesses or vulnerabilities could allow unauthorised users to gain direct and public access to the backend databases in order to churn sensitive and valuable information, which might cause significant damage to the system.

This special issue aims at documenting state-of-the-art research, new developments and directions for future investigations in the security issues in internet and web applications. We received a good number of high quality manuscripts from all over the globe, of which only ten papers have been selected for this special issue after a rigorous and thorough review and revision process. The selected papers address different critical challenges in the security issues for internet and web applications and broadly fall into different categories including theoretical modelling, design and analysis of security schemes in the relevant areas.

The paper 'A formal framework to support dynamic authorisation in collaborative environments' by Simeon Veloudis, Dimitrios Baltatzis, Christos Ilioudis and George Pangalos, studies the security problem in online collaborative environments. This paper proposes a formal

model to provide a practical role assignment methodology between organisations in collaboration, taking into account organisational as well as functional characteristics. The applicability of the formal framework is investigated through a realistic case study.

Distributed denial of service (DDoS) attacks pose a significant threat to the internet. Aiming to address this security problem, Zakaria Al-Qudah, Basheer Al-Duwairi and Osama Al-Khaleel present a paper entitled 'DDoS protection as a service: hiding behind the giants', which proposes a content distribution network (CDN)-based DDoS protection service to counter attacks targeting application layer of web servers. The proposed scheme is evaluated through extensive experiments over Planetlab.

He Du, Jian Wang and Ya-Nan Liu present the paper 'Independent verification of proxy multi-signature scheme', which proposes a special secure proxy multi-signature scheme with independent verification property. In this scheme, after the proxy signer finishes proxy multi-signature, others can verify it using the public keys of the special original signers whom he wants to verify, rather than using all the proxy signers' public keys. This scheme can be used in a scenario where the proxy signer hopes to make the verifier verify the signature with only the public keys of the special original signers while the others are kept secret. This article is interesting given the idea presented and could be more suitable for the experts in the relevant fields.

PubKey-Wiki incorporates public key security into a wiki group collaboration system. PubKey-Wiki introduced a certificate closure algorithm that computes the transitive closure of a set of certificates that contain authorisation information. The paper 'Hybrid certificate closure-chain discovery public key system' by Dwaine Clarke introduces a hybrid PubKey-Wiki system that combines both the certificate closure algorithm and a certificate chain discovery algorithm in a new architecture that leverages the strengths of both algorithms.

Online social networks (OSNs) are a very popular phenomenon now-a-days to provide a cyber social environment. The heterogeneous deployment of OSNs, along with intrinsic sharing of personal information, leads to severe risks both in terms of security and privacy. With the aim of addressing this issue, the paper 'A taxonomy-based model of security and privacy in online social networks' by L. Caviglione, M. Coccoli and A. Merlo, proposes a taxonomy-based approach to describe and model the complex security space characterising OSNs. This paper introduces a systematic approach to define the problem space of an OSN and exhibits basic models for organising the engineering and the necessary checking procedures.

In the paper 'A lightweight possession proof scheme for outsourced files in mobile cloud computing based on chameleon hash function' by Wei Ren and Yuliang Liu, a family of possession proof schemes are proposed for the integrity check of outsourced storage in mobile cloud environment. The proposed advanced scheme is lightweight, supports mobility, and cooperativeness in mobile cloud computing. The evaluation of security and performance is extensively analysed, which justifies the applicability of the proposed scheme.

The paper 'Modelling the relationship between trust and privacy in network environments' by Feng Gao, Jingsha He and Shunan Ma, studies the relationship between trust and privacy in network environments based on game theory which considers the factor of the privacy owner's lying to the interactive entity. This paper also shows how the proposed model can be applied in network interactions between entities through some application scenarios.

Mobile payments require the ability to make payments with the help of a mobile handset anytime, anywhere and for any reason; hence, end to end security is very important for mobile payments. Considering this fact, Shaik Shakeel Ahamad, V.N. Sastry and Siba K. Udgata present the paper 'Secure mobile payment framework based on UICC with formal verification', which proposes a secure mobile payments framework based on universal integrated circuit card (UICC) by defining

a a procedure of personalising UICC by the client

b a procedure of provisioning and personalisation (mutual authentication and key agreement protocol) of mobile payments application (which is on UICC) by the bank

c a mobile payment protocol between the personalised mobile payment application on UICC and the bank server.

The proposed protocols have been verified using BAN logic and Scyther tool. Burrows-Abadi-Needham logic (also known as the BAN logic) is a set of rules for defining and analysing information exchange protocols. Specifically, BAN logic helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both.

The paper 'Robust multichannel colour image watermarking using lifting wavelet transform with singular value decomposition' by Sushma G. Kejgir and Manesh B. Kokare, proposes a new multichannel colour image watermarking for copyright protection in multimedia applications using lifting wavelet transform (LWT) and singular value decomposition (SVD) technique. The proposed algorithm is tested for robustness against benchmark Stir Mark 4.0 standard attacks on different images.

Al-Sakib Khan Pathan and Diallo Abdoulaye Kindy, in their paper 'Lethality of SQL injection against current and future internet-technologies', present easily accessible information about SQL injection against current and future internet technologies and networks, which is commonly termed as a kind of *hacking* very well spread today. This paper presents the insights of various forms of SQL injection attacks and analyses how these techniques could be applied in the future networks technologies. They identify that, as the core mechanism of backend databases would remain more or less the same, the underlying threats

would also remain almost the same via different methods of communications. Hence, they suggest that the awareness of the latest trends, fixing loopholes when exposed, defensive operations, constant monitoring, and continuous learning as the best defence against all the explored attacks.

A special issue like this could not have been prepared without the efforts of many people who are not mentioned here. First, we want to thank the referees for their invaluable service who provided timely and constructive feedback to the authors. Second, we want to acknowledge the tremendous interests of the authors in this special issue. We hope that the authors of the papers that we could not include in this issue will continue developing their works further based on the review comments. Third, our deepest gratitude and special thanks must go to the Editor-in-Chief of *IJCSE*, Dr. Kuan-Ching Li, for supporting the launch of this Special Issue. Finally, we would like to thank very much the editorial office staff of the *IJCSE* and Inderscience publishers for all of their help and support throughout the preparation process of this issue.