PREFACE

Future Trends in Security Issues in Internet and Web Applications

The massive proliferation of Web applications is 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 Internet is the implemented networking infrastructure that connects millions of computers together which could be located 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 unauthorized users to gain direct and public access to the backend databases in order to churn sensitive and valuable information which might cause significant damages 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 modeling, design and analysis of security schemes in the relevant areas.

The paper, “A Formal Framework to Support Dynamic Authorization in Collaborative Environments” by Simeon Veloudis, Dimitrios Baltatzis, Christos Ilioudis, and George Pangalos, studies the security problem in on-line collaborative environments. This paper proposes a formal model to provide a practical role assignment methodology between organizations in collaboration taking into account organizational 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 CDN (Content Distribution Network)-based DDoS protection service to counter attacks targeting application layer of web servers. The proposed scheme is evaluated through extensive experiments over Planetlab.

Du He, Wang Jian, and Liu Ya-nan present the paper "Independent Verification of Proxy Multi-signature Scheme" that 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 keeps others 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 the CertClosure algorithm that computes the transitive closure of a set of
certificates which contain authorization information and architecture. In the paper, "Hybrid
Certificate Closure-Chain Discovery Public Key System", by Dwaine Clarke, a hybrid PubKey-
Wiki system is introduced that combines both the certificate closure algorithm and a certificate
chain discovery algorithm in a new architecture which leverages the strengths of both algorithms.

Online Social Networks (OSNs) are a very popular phenomenon now-a-days to provide cyber
social environment. The heterogeneous deployment of OSNs along with intrinsic sharing of
personal information lead 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 Mauro Coccoli, Luca Caviglione, and Alessio Merlo, proposes a
taxonomy-based approach to describe and model the complex security space characterizing
OSNs. This paper introduces a systematic approach to define the problem space of an OSN and
exhibits basic models for organizing the engineering and the needed 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 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 are
extensively analyzed, which justifies the applicability of the proposed scheme.

The paper, "Modeling the Relationship between Trust and Privacy in Network Environments"
by Gao, Jingsha He, and 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 much important for
mobile payments. Considering this fact, Shakeel Shaik, Sastry V.N., 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 personalizing UICC by the client, (b) a procedure of
provisioning and personalization (Mutual Authentication and Key Agreement Protocol) of
Mobile Payments Application (which is on UICC) by the Bank, and (c) a mobile payment
protocol between the personalized 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 analyzing
information exchange protocols. Specifically, BAN logic helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both.

The paper, "Robust Multichannel Color Image Watermarking using Lifting Wavelet Transform with Singular Value Decomposition" by Sushma Kejgir and Manesh Kokare proposes a new multichannel color 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 analyzes 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 defense 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 staffs of the IJCSE and Inderscience publishers for all of their help and support throughout the preparation process of this issue.

Guest Editors

Al-Sakib Khan Pathan
Department of Computer Science,
International Islamic University Malaysia,
Gombak, Kuala Lumpur, Malaysia.
spathan@ieee.org, sakib@iium.edu.my

Muhammad Mostafa Monowar
Department of Information Technology,
King AbdulAziz University,
Jeddah, Kingdom of Saudi Arabia.
hemal.cu@gmail.com, monowar@ieee.org