Gupta et al. EURASIP Journal on Information Security (2016) 2016:27
DOI 10.1186/s13635-016-0051-2

EURASIP Journal on Information Security

EDITORIAL Open Access

Guest editorial special issues on security trends in mobile cloud computing, web, and social networking

B. B. Gupta[1*], Shingo Yamaguchi[2] and Pethuru Raj Chelliah[3]

Internet security has become an independent branch of computer security dealing with the Internet, and often involves applications or operating systems as a whole besides browser security. The sole objective is to establish rules that can be used against potential attacks [1]. Moreover, cyber security is an essential need for modern society where information technology and services pervade every aspect of our lives. However, it is challenging to achieve, as technology is changing at rapid speed and our systems turn into ever more complex. We are gradually more dependent upon such information and communications infrastructures, and the threats we face are organized and exploit our dependency by the attackers or cyber criminals. Moreover, cyber space is considered as the fifth battlefield after land, air, water, and space [2]. Mobile cloud computing, web and social networking have gained more and more attention in recent years. There are still significant security challenges in the development of cloud infrastructure, web, and mobile terminal devices. This special issue addresses various security issues in social networking, web, and cloud computing, particularly on advances in mobile computing technologies and related areas [3, 4].

This special issue contains five papers dealing with different aspects of security issues in social networking, web, and cloud computing and other related areas. The first article entitled "Experimental comparison of simulation tools for efficient cloud and mobile cloud computing applications" co-authored by Khadijah Bahwaireth et al. [5] presents experimental comparison of various simulation tools and shows how these simulation tools can be used for efficient cloud and mobile cloud computing applications. They considered CloudSim, CloudAnalyst, CloudReports, CloudExp, GreenCloud, and iCanCloud simulation tools for their study. Moreover, authors have also performed experiments using some of these simulation tools to show their capabilities and effectiveness.

The second paper entitled "An adaptive approach for Linux memory analysis based on kernel code reconstruction" authored by Shuhui Zhang et al. [6] presents an adaptive approach for Linux memory analysis that can automatically identify the kernel version and recovery symbol information from an image. The proposed approach is able to automatically reconstruct the kernel code, identify the kernel version, recover symbol table files, and extract live system information by providing a memory image or a memory snapshot only. There is no other information required for it. Various experiments are performed and results indicate that proposed approach runs satisfactorily across a wide range of operating system versions.

The third paper entitled "A secure cloud storage system combining time-based one-time password and automatic blocker protocol" authored by Sheren A. El-Booz et al. [7] presents a novel secure cloud storage system to ensure the protection of organizations' data from the cloud provider, the third party auditor, and some users who may use their old accounts to access the data stored on the cloud. There are two authentication techniques used in the proposed system to improve the authentication level of security. (i) Time-based one-time password (TOTP) for cloud users verification and (ii) automatic blocker protocol (ABP) to fully protect the system from unauthorized third party auditor. Various experiments are performed and results prove the effectiveness and efficiency of the proposed system when auditing shared data integrity.

The fourth paper entitled "Generalized weighted tree similarity algorithms for taxonomy trees" is authored by Pramodh Krishna D. et al. [8]. In this paper, authors introduce a generalized formula to combine matching and missing values. Subsequently, authors proposed two generalized weighted tree similarity algorithms. The first

* Correspondence: gupta.brij@gmail.com
[1]National Institute of Technology Kurukshetra, Kurukshetra, India
Full list of author information is available at the end of the article

algorithm calculates matching and missing values between two taxonomy trees separately and combines them globally. The second algorithm calculates matching and missing values at each level of the two trees and combines them at every level recursively which preserves the structural information between the two trees. The missing value in similarity computation is efficiently used in the proposed algorithms in order to distinguish among taxonomy trees that have the same matching value but with different miss trees at different positions. Finally, authors have generated a set of synthetic weighted binary trees and performed various experiments that prove the effects of arc weights, matching as well as missing values in a pair of trees.

The fifth paper entitled "A novel approach to protect against phishing attacks at client side using auto-updated white-list" authored by Ankit Kumar Jain et al. [9] presents a novel approach to protect against phishing attacks using auto-updated white-list of legitimate sites accessed by the individual user. The proposed approach checks the legitimacy of a webpage using hyperlink features. Therefore, various hyperlinks (and features from the hyperlinks) from the source code of a webpage are extracted and apply to the proposed phishing detection system. Authors have performed various experiments and results show that the proposed approach is very effective in detecting and protecting against phishing attacks. Proposed approach has 86.02 % true positive rate while less than 1.48 % false negative rate. Moreover, various other types of phishing attacks (i.e., domain name system (DNS) poisoning, embedded objects, zero-hour attack) can also be detected efficiently using the proposed approach.

This special issue is due to encouragement of Dr. Stefan Katzenbeisser who is instrumental in the organization process. Many individuals have contributed for success of this issue. Special thanks are due to dedicated reviewers who found time from their busy schedule to review the articles submitted in this special issue. This special issue presents some selected papers in touching important aspects of security in the social networking, web, and cloud computing, particularly on advances in mobile computing technologies and related areas, and also emphasizes many open questions. The widespread use of social networking, web, and cloud computing is encouraging researchers to look at various open questions, and a lot more work need to be done before it becomes a reality and widely accepted by the user community.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]National Institute of Technology Kurukshetra, Kurukshetra, India. [2]Yamaguchi University, Yamaguchi, Japan. [3]IBM Global Cloud Center of Excellence (COE), IBM, Bangalore, India.

Received: 5 October 2016 Accepted: 5 October 2016
Published online: 08 November 2016

References

1. P Gralla, *How the Internet Works* (Que Pub, Indianapolis, 2007). ISBN 0-7897-2132-5
2. BB Gupta, DP Agrawal, S Yamaguchi, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (IGI Global Publisher, USA, 2016)
3. D.P. Agrawal, Q-A. Zeng, *Introduction to Wireless and Mobile Systems*, 4th edn, Cengage Learning, 2016
4. M. O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*, Apress, 2015
5. K Bahwaireth et al., Experimental comparison of simulation tools for efficient cloud and mobile cloud computing applications. EURASIP J. Inf. Secur. **2016**(1), 1–14 (2016)
6. S Zhang, X Meng, L Wang, An adaptive approach for Linux memory analysis based on kernel code reconstruction. EURASIP J. Inf. Secur. **2016**(1), 1–13 (2016)
7. SA El-Booz, G Attiya, N El-Fishawy, A secure cloud storage system combining time-based one-time password and automatic blocker protocol. EURASIP J. Inf. Secur. **2016**(1), 1–13 (2016)
8. DP Krishna, K Venu Gopal Rao, Generalized weighted tree similarity algorithms for taxonomy trees. EURASIP J. Inf. Secur. **1**(2016), 35 (2016)
9. AK Jain, BB Gupta, A novel approach to protect against phishing attacks at client side using auto-updated white-list. EURASIP J. Inf. Secur. **2016**(1), 1–11 (2016)