J Comput Virol Hack Tech (2015) 11:119–121
DOI 10.1007/s11416-015-0248-9

EDITORIAL

Convergence security systems

Sang-Yeob Oh[1] · Supratip Ghose[2] · Yu-Keum Jeong[3] · Joong-Kyung Ryu[4] · Jungsoo Han[5]

Published online: 21 July 2015

Convergence-based service environments are embedded in large-capacity servers and adopt client/server models. Applications, devices, networks, and infrastructure are converging and creating an immense amount of content, which poses complex challenges for organizations, developers and users. In the field of security, we are seeing the convergence of frameworks and paradigms like augmented reality, ubiquitous computing and pervasive computing; and we are seeing new kinds of content, much of it user-generated, that can be searched, organized and consumed on many devices and in many formats [10–15]. The challenges of converged security, hacking, computer virology technologies and content require new algorithms, application paradigms, interaction methods, and services; the creation of expressive annotation frameworks, scalable algorithms, and new paradigms for information discovery; and ways of searching, organizing and delivering converged information for delivery at the right place, at the right time and at the right level of detail. This special focus issue on convergence security systems will address the need for novel services and reviews security vulnerabilities in recent years. Some of these research areas are listed below.

- Privacy and authentication for wireless networks
- Convergence security in ubiquitous computing
- Algorithmic and computer virology
- Innovative applications in ubiquitous computing
- Intelligent applications for multimedia processing
- Hacking; computer virology
- User experience with convergence systems
- Personalization, security and privacy
- Information indexing, searching, and visualization
- Intelligent information processing algorithms
- Sensors, wireless technology and embedded systems
- Applications in computer virology

This special issue is devoted to one of the hottest topics in convergence security systems, and its articles are expected to be cited widely in the areas of computer virology and hacking techniques.

Lee et al. [1] present reconfigurable real number–field elliptic curve cryptography to improve security. They propose a method for configuring a cryptographic system using real number–field coordinates on an elliptic curve, as well as a finite field, through expansion of existing elliptic curve cryptography. They discuss a method for application of an elliptic curve defined on a real-number field for cryptographic systems and the advantages obtained from the use of a real-number field. Hong [2] introduces an efficient and secure

✉ Jungsoo Han
jungsoo.han.k@gmail.com

Sang-Yeob Oh
syoh@gachon.ac.kr

Supratip Ghose
sgresearch@gmail.com

Yu-Keum Jeong
digital@policy.or.kr

Joong-Kyung Ryu
jkryu@daelim.ac.kr

1 Department of Interactive Media, Gachon University, Seongnam, Republic of Korea

2 Department of Computer Science and Engineering, University of Information Technology and Sciences, Dhaka, Bangladesh

3 Strategy Department, Society of Digital Policy and Management, Seoul, Republic of Korea

4 Department of Computer Software, Daelim University, Anyang, Republic of Korea

5 Division of Information and Communication, Baekseok University, Cheonan, Republic of Korea

domain name server (DNS) cyber shelter from distributed denial of service (DDoS) attacks. This study proposes a DNS cyber shelter that can detect DDoS attack packets and block their source. In computer security, a demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.

Jeong et al. [3] present a token-based authentication security scheme for a Hadoop distributed file system using elliptic curve cryptography. They propose a token-based authentication scheme that protects sensitive data stored in a Hadoop distributed file system (HDFS) against replay and impersonation attacks. The proposed scheme allows HDFS clients to be authenticated by a data node via block access token. Unlike most HDFS authentication protocols adopting public key exchange approaches, the proposed scheme uses the hash chain of keys. The proposed scheme offers performance (communication power, computing power and area efficiency) as good as that of existing HDFS systems. Lee et al. [4] look at the vulnerabilities of intelligent automobiles using TPEG (Transport Protocol Expert Group) updates based on T-DMB and its countermeasures. They propose security countermeasures (after creating an attack scenario in order to transmit the update information) that are reliable by identifying the characteristics of the wireless update for navigation. In the scenarios proposed, they derive a navigation attack scenario through an analysis of T-DMB and TPEG and propose countermeasures to the derived security threats in order to propose a security system that can defend against the attack.

Lee [5] introduces a secure authentication scheme for a smart learning system in a cloud computing environment. The authentication scheme allows users to securely have access to a smart learning system in a cloud environment. The method he proposes is safe against user information leaks because it stores the user information through a hash-chain when a registered user's USIM_ID is granted access to the proposed scheme. Im et al. [6] present banking behavior in security and multi-channel environments. They propose differences of factors affecting banking behavior in a multi-channel environment. This paper adopted multi-group structural equation modeling to compare the differences in causalities between internet and mobile banking. The result of causality supports the theory of the technology acceptance model, and the paths across the two groups are different.

Jo et al. [7] present an efficient thread partition policy for secure functional language. They propose an enhancing thread partition policy, which is the most significant part when a non-strict function program is translated in order to efficiently materialize function language in a multithread model. A thread partition policy algorithm is proposed in order to enhance the efficiency of an existing thread partition performing thread partition by analyzing the dependence relationship between operations in a non-strict function program. Shin et al. [8] present an association analysis of technology convergence based on information system utilization. They propose figuring out convergence technology fields using an analysis of utilization patterns in academic papers or patent information that is used together by researchers. This study deduces convergence utilization between technologies by analyzing the relationships between the fields of information utilized simultaneously through an analysis of the usage sessions of NDSL (National Digital Science Library of Korea). Choi [9] introduces a study on model fostering for a cloud service brokerage (CSB). This study proposes a brokerage CSB development model, and suggests policy measures that apply to co-operation in cloud service business models. Cloud service brokerage is a traditional service, and solutions produced by a variety of cloud services' adoption of asset management, service level agreements (SLAs) interdependence management, compliance management, risk management and security solutions are presented for complex issues.

This fine collection of papers was accumulated by fruitful collaboration. We gratefully acknowledge and express our heartfelt appreciation to all the authors for their excellent contributions to this special issue. We would also like to thank all the members of the SDPM, ICDPM Program Committee and anonymous reviewers for their help in identifying novel papers and for their careful reading of earlier drafts to select 9 high-quality papers out of 25 papers submitted—a 36 % acceptance rate. Furthermore, we would like to thank Professor Eric Filiol, editor-in-chief of the *International Journal of Computer Virology and Hacking Techniques*, for his valuable remarks and help throughout the publication process of this special issue.

References

1. Goo, E.H., Lee, S.D.: Reconfigurable real number field elliptic curve cryptography to improve the security. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-014-0233-8 (2014)
2. Hong, S.: Efficient and secure DNS cyber shelter on DDoS attacks. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-014-0230-y (2014)
3. Kim, Y.T., Jeong, Y.S.: A token-based authentication security scheme for Hadoop distributed file system using elliptic curve cryptography. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-014-0236-5 (2015)
4. Kim, J.H., Lee, K.H.: Vulnerabilities of intelligent automobiles using TPEG update based on T-DMB and its countermeasures. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-015-0243-1 (2015)
5. Lee, A.: Authentication scheme for smart learning system in the cloud computing environment. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-015-0240-4 (2015)
6. Lee, S.C., Im, K.H.: Banking behavior in security and multi-channel environment. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-014-0235-6 (2015)

7. Jo, S.M., Chung, K.: An efficient thread partition policy for secure functional language. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-014-0234-7 (2014)
8. Shin, S., Yoo, S., Kim, H., Lee, T.: Association analysis of technology convergence based on information system utilization. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-015-0238-y (2015)
9. Choi, S.: Study on model fostering for cloud service brokerage. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-015-0246-y (2015)
10. Boutaba, R., Chung, K., Gen, M.: Recent trends in interactive multimedia computing for industry. Cluster Comput. **17**(3), 723–726 (2014)
11. Chung, K., Boutaba, R., Hariri, S.: Recent trends in digital convergence information system. Wirel. Personal Commun. **79**(4), 2409–2413 (2014)
12. Oh, S.Y., Chung, K.Y.: Target speech feature extraction using non-parametric correlation coefficient. Cluster Comput. **17**(3), 893–899 (2014)
13. Kim, J.H., Ryu, J.K.: Recent trends on high-performance computing and security. Cluster Comput. **16**(2), 207–208 (2013)
14. Han, J.: Distributed hybrid P2P networking systems. Peer Peer Netw. Appl. **8**(4), 555–556 (2015)
15. Kim, J.H., Ryu, J.K.: Recent trends on high-performance computing and security. Cluster Comput. **16**(2), 207–208 (2013)