J Comput Virol Hack Tech (2017) 13:239–240
DOI 10.1007/s11416-017-0311-9

EDITORIAL

Hacking and convergence computing

Sunkyung Rhyu[1] · **SangYeob Oh**[2]

Published online: 29 October 2017

Recently, in terms of the use of Internet of Things (IoT) devices in the smart platform for security management, companies have been releasing diverse products, and such products are being proved as effective in the continuous management of computer virology. In addition, in the field of security services, companies and research institutes have been continuously developing solutions using hacking and convergence computing [10–12]. This issue covers some of the hottest topics in hacking and convergence computing, including: hacking in convergence computing; electronics hacking, hardware hacking; communication protocol hacking; information indexing, searching, and visualization; secure and anti-hacking; network connection solution; secure virtual network embedding algorithms; secure information authentication protocol; security framework; secure IoT and protocol; privacy and authentication for network; security in convergence computing; cybersecurity; innovative applications of hacking, security computing.

The paper by Hong [1] presents a secure and light IoT protocol (SLIP) for antihacking. The proposed method introduces a number of typical applications such as the smart home, intelligent transportation, a security-issue analysis, and related convergence technologies for the realization of a secure IoT. Further, a comparison of the security issues between the IoT and the traditional network was performed, and it was concluded that the environment of the IoT-convergence system is a dangerous one with limited resources and fewer network guards. The paper by Li et al. [2] analyzes a study on the service and the trend of fintech security that is based on text mining. This study presents the tasks and directions of the fintech industry in consideration of the successful operation of fintech security through an analysis of the news articles from an online-data collection. The results contributed to a switching of the market awareness of fintech services and security in the present-day ongoing expansion of the fintech market.

The paper by Bang [3] introduces the research on financial-institution network-partition design for antihacking. The proposed solution comprises management efficiency, a data-system safety-operation solution, an optimized network-separation system that is developed through the integration of a conventional security system, and a new establishment and process in the financial field. This is a security measure that is supported by the appropriate security of the memory devices for which the minimally required security measure is applied. The paper by Kim et al. [4] presents an evaluation method for secure virtual-network embedding algorithms. This is the Virtual Network Embedding Evaluation Method (VNE-EM) that can be used for purposes such as security, energy efficiency, and mobility functionality. They analyzed a number of studies, and they found appropriate evaluation indexes that can be used in an evaluation of the functionalities of VNE (virtual network embedding) algorithms, for which a grouping of the functional attributes is performed for a real-time classification. The proposed method is more convenient for the performance of the evaluation of the algorithms of infrastructure providers.

The paper by Jeong [5] presents a secure information-authentication protocol that concerns the relationship

✉ SangYeob Oh
syoh.gc@gmail.com

Sunkyung Rhyu
sunkyung.rhyu@gmail.com

[1] Strategy Department, Korea Convergence Society, Daewoo Plaza 301, Dujeong-ro 240, Cheonan-si, Chungcheongnam-do, Republic of Korea

[2] Department of Computer Engineering, Gachon University, Bokjeong-dong, Sujeong-gu, Seongnam-si, Gyeonggi-do 461-701, Republic of Korea

between the patients and the medical staff in a hospital environment. This paper presents a mandate-based signature-authentication protocol that delivers the personal information for the provision of medical services, where access is given in a wireless network to only the staff members who care for the patient. All accesses are inspected by the authentication servers to prevent third parties from gaining access to the sensitive biometric data of patients, and the servers protect against the disguised proxies of attackers. The paper by Yoo et al. [6] proposes a context-aware-based user-customized light-therapy service using the security framework. This study presents a context-aware-based security framework to enhance the real-time security of personal-health services for the interlocking that can protect medical information by complying with the standard-based security guideline, encryption. This is a component of the DOGF (Distributed Object Group Frame) for the management of the security of the health domain and the health level 7 (HL7), which can be reformed depending on the security-requirement situation.

The paper by Park et al. [7] introduces a performance evaluation of the information-security training in the public sector. For this study, an analysis of the outcomes of education and training in the field of information security was performed, and the economic return on investment was assessed based on the training programs and the sustainability of the training centers. Also, this contributed to the development of highly skilled information-security personnel by improving the quality of the training programs. The paper by Jo [8] introduces a secure access policy for efficient resource management in the mobile-computing environment. This study presents a secure access-policy method for query processing to enable efficient resource management for the dynamic XML-data access in a mobile environment, where the authority and a secure access for the reading of specific information in the element, add, and search along the link, delete, and modify element links in a mobile environment are provided. Finally, the paper by Kong et al. [9] suggests the implementation of a dataset-staging process with improved security in a new analytic facility for the ALICE experiment. ALICE (A Large-Ion Collider Experiment) is a general-purpose, heavy-ion detector at the Large Hadron Collider (LHC) computing-grid project. The ALICE experiment provides a single access point to the LHC Grid through a framework. The researchers presented a facility for both the business and scientific-research areas that supports a research group and provides "on-the-fly" random access to the data that are remotely distributed throughout the Grid.

We would like to thank Editors-in-Chief Professor Eric Filiol of Computer Virology and Hacking Techniques journal and all office staffs for their valuable supports throughout the publication of issue.

References

1. Hong, S.: Secure and light IoT protocol (SLIP) for anti-hacking. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0295-5
2. Li, G., Dai, J.S., Park, E.M., Park, S.T.: A study on the service and trend of Fintech security based on text-mining: focused on the data of Korean online news. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-016-0288-9
3. Bang, S.W., Jung, B.S., Lee, S.C.: Research on financial institutional network partition design for anti-hacking. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0297-3
4. Kim, H.S., Lee, S.H.: An evaluation method for secure virtual network embedding algorithms. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0303-9
5. Jeong, Y.S.: Secure information authentication protocol between patients and medical staff in a hospital environment. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0294-6
6. Yoo, H., Kim, J.C., Kim, K.W., Park, R.C.: Context aware based user customized light therapy service using security framework. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0298-2
7. Park, S.K., Lee, S.H., Kim, T.Y., Jun, H.J., Kim, T.S.: A performance evaluation of information security training in public sector. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0305-7
8. Jo, S.M.: Secure access policy for efficient resource in mobile computing environment. J. Comput. Virol. and Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0301-y
9. Ahn, S.U., Park, S.O., Kim, J.H., Kong, B.: Implementation of dataset staging process with improved security in a new analysis facility for ALICE experiment. J. Comput. Virol. Hacking. Tech. (2017). https://doi.org/10.1007/s11416-017-0308-4
10. Chung, K., Boutaba, R., Hariri, S.: Knowledge-based decision support systems. Inf. Technol. Manag. **17**(1), 1–3 (2016)
11. Rhyu, S., Oh, S.Y.: ICT-based wireless personal computing. Wirel. Pers. Commun. **93**(1), 1–5 (2017)
12. Oh, S.Y., Chung, K., Han, J.S.: Towards ubiquitous health with convergence. Int. J. Technol. Health Care **24**(3), 411–413 (2016)