Editorial
Special Issue on "Selected Papers from MobiSec 2016"

Ilsun You[1], Hsing-Chung Chen[2,3], Fang-Yie Leu[4]

[1] Department of Information Security Engineering, Soonchunhyang University, South Korea
[2] Asia University, Taiwan
[3] China Medical University Hospital, China Medical University, Taiwan
[4] Department of Computer Science, TungHai University, Taiwan
ilsunu@gmail.com, cdma2000@asia.edu.tw, shin8409@ms6.hinet.net, leufy@thu.edu.tw

During the past two decades, mobile Internet technologies have been dramatically growing while leading to a paradigm shift in our everyday life. Despites their revolution, mobile Internet technologies also open doors to various security threats, which should be addressed to keep mobile Internet environments to be secure and trustable. Even worse, the latest technologies, e.g. distributed mobility management, mobile Internet of things, 5G networks, and so forth, are continuously introducing new security challenges. Therefore, it is of paramount importance to study mobile Internet security.

Topics of this special issue include new security vulnerabilities and threats in mobile internet and networks, security issues and protocols for mobile internet and networks, privacy and trust for mobile internet and networks, security for cross-layer handover, security for vertical handover in heterogeneous networks, security for 4G and 5G networks, security for IoTs and wearable devices, security for mobile internet services and applications, advances in mobile internets and networks, security for Big data and Cloud environments, security for quantum key distribution, security for wireless sensor networks and other emerging new topics.

To this Special Issue were selected ten articles of particular interest, as they present the most interesting researches within the subject matter of this special issue.

The paper "Multi-Partitioned Bytecode Wrapping Scheme for Minimizing Code Exposure on Android" by Park et al. [1] presented the scheme that makes reverse engineering analysis difficult. It was achieved by wrapping and dropping the original bytecode after separating the original bytecode, thereby resolving the problem of exposing all the original bytecodes. In addition, their proposed scheme could be applied to a sample application. Finally, the security and performance of the proposed scheme were compared with those of existing techniques.

The paper entitled "Moving Deferrable Big Data to the Cloud by Adopting an Online Cost-Minimization Approach" by Cui et al. [2] discussed how to use the allowable delay window to reduce peak volume by increasing the maximum transmission of early stages. Their experiments showed that the peak value could be reduced by choosing a larger initial value. Besides, they also discussed how to assign workloads among data centers in the cloud scenario. Finally, the total bandwidth cost of data centers could be minimized when the maximum transmission capacity of these data centers are generally equal to each other.

The paper entitled "A Universal Quantum Key Distribution Simulation Method Towards Future Internet" by Peng et al. [3] presented a simulation method for the physical subsystem of quantum communication network. In this method, they partitioned the physical devices of the quantum communication network into three modules: single photon source, quantum channel and single photon detector. In addition, they divided the quantum channel into fiber channel and free-space channel. The mathematical models were established for physical devices and quantum channels, so that they could calculate the loss and efficiency of different modules according to the parameters of the actual equipment, and finally get the simulation data closed to the output of the real physical equipment. Therefore, their simulation method could be applicable to different quantum communication networks. Unlike previous theoretical based studied, they could get the simulated output, and their simulated results could be used as the raw key.

The paper entitled "Authorized client-side deduplication using access policy-based convergent encryption" by Youn et al. [4] presented the method to provide efficient use of cloud storage while supporting secure data sharing in the cloud. In order to provide authorized deduplication, they used the convergent encryption scheme and applied an access privilege to generate a convergent key. Because of this, the user without proper privileges will not be able to generate

*Corresponding Author: Ilsun You; E-mail: ilsunu@gmail.com

the convergent key and thus cannot access the shared data. To verify the ownership of the file in the client-side deduplication procedure, they also proposed a new proof of ownership protocol based on an existing Merkle tree-based protocol. Their scheme provided an adequate trade-off between security and storage space efficiency. By executing the deduplication for users with the same privilege, the effect of deduplication could be reduced. However, in view of the data sharing, their approach has the advantage in the sense that only authorized users could access the files encrypted based on privileges allowed to the authorized users. The proposed scheme is very suitable for the hybrid cloud model considering both the data security and the storage efficiency.

The paper entitled "Performance of Improved Fuzzy Indoor Zone Positioning Systems in Wireless Sensor Networks" by Cheng et al. [5] presented the zone-based indoor positioning scheme using a wireless sensor networks (WSNs) in conjunction with a fuzzy-based algorithm. The authors discussed how to use the received signal strength indicator (RSSI) to determine the distance between the target node and referenced nodes in indoor environments. This technique with propagation characteristic had previously been used to construct a signal propagation channel model. In this proposed scheme, the RSSI is divided into several power levels based on the rate of signal attenuation over distance, and the indoor environment is splitting up into some zones. A fuzzy inference system (FIS) algorithm proposed in this scheme is used to improve the accuracy of localization. The RSSI values from several reference nodes will be used as inputs in the FIS to estimate the location of the target node within a zone. Finally, their simulation results showed that the fuzzy rectangular splitting method is the most suitable approach to splitting up the zone.

We believe that all papers included in this Special Issue will have a special importance for future scientific research works, and also make the contributions to the studies conducted by other researchers and engineers, who work in advanced mobile security technologies. We would like to express our sincere appreciation of the valuable contributions made by all authors. Our special thanks go to President Han-Chie Chao, the Editor-in-Chief of the Journal of Internet Technology (JIT), for allowing us to publish this Special Issue, and for his highly supports throughout the entire publication process.

References

[1] Y. Park, T. Park, J. H. Yi, *Multi-Partitioned Bytecode Wrapping Scheme for Minimizing Code Exposure on Android*, JIT-SI-2017-0062.R1.

[2] B. Cui, X. Jin, P. Shi, *Moving Deferrable Big Data to the Cloud by Adopting an Online Cost-Minimization Approach*, JIT-SI-2017-0063.R1.

[3] Y. Peng, B. Liu, B. Zhao, C. Wu, W. Yu, *A Universal Quantum Key Distribution Simulation Method Towards Future Internet*, JIT-SI-2017-0064.R1.

[4] T.-Y. Youn, K.-Y. Chang, K. H. Rhee, S. U. Shin, *Authorized Client-side Deduplication Using access Policy-based Convergent Encryption*, JIT-SI-2017-0065.R1.

[5] C.-H. Cheng, Y. Yan, Y.-F. Huang, *Performance of Improved Fuzzy Indoor Zone Positioning Systems in Wireless Sensor Networks*, JIT-SI-2017-0067.R1.

Guest Editors

Ilsun You received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, Korea, in 1997 and 2002, respectively. He received the second Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was at the THINmultimedia Inc., Internet Security Co., Ltd. and Hanjo Engineering Co., Ltd. as a research engineer. Now, he is an associate professor at Department of Information Security Engineering, Soonchunhyang University. He has served or is currently serving as a main organizer of international conferences and workshops such as MIST, MobiSec, MobiWorld, and so forth. Dr. YOU is the EiC of Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). He is in the Editorial Board for Information Sciences (INS), Journal of Network and Computer Applications (JNCA), IEEE Access, Intelligent Automation & Soft Computing (AutoSoft), International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Computing and Informatics (CAI), and Journal of High Speed Networks (JHSN). Especially, he has published more than 180 papers in his main areas including internet security, IoT, 4G/5G security, wireless & mobile networks, and so forth. He is a Fellow of the IET and a Senior member of the IEEE.

Hsing-Chung Chen received the Ph.D. degree in Electronic Engineering from National Chung Cheng University, Taiwan, in 2007. During the years 1991-2007, he had served as a Mobile Communication System Engineer at the Department of Mobile Business Group, Chunghwa Telecom Co., Ltd. From Feb. 2008 to Feb. 2013, he was the Assistant Professor of the Department of Computer Science and Information Engineering at Asia University, Taiwan. Since February 2013–present, he is the Associate Professor of the Department of Computer Science and Information Engineering at Asia University, Taiwan. Since May 2014–present, he is also the Research

Consultant of Dept. of Medical Research, China Medical University Hospital, China Medical University Taichung, Taiwan. In addition, since Feb 2015–present, he is the Permanent Council Member of Taiwan Domain Names Association (Taiwan DNA), Taiwan. Currently, his current research interests include Cryptography, Role-based Access Control, Information and Network Security, Mobile and Wireless Communications, and Bioinformatics Signal Processing. He is the members of CCISA, ICCIT, IET and IEEE. He had received the MobiSec2017 and BWCCA2016 Best Paper Award, individually.

Fang-Yie Leu received his B.S., M.S. and Ph.D. degrees from National Taiwan University of Science and Technology, Taiwan, in 1983, 1986 and 1991, respectively, and another M.S. degree from Knowledge Systems Institute, USA, in 1990. His research interests include wireless communication, network security, Grid applications and Chinese natural language processing. He is currently a workshop organizer of CWECS and MCNCS workshops, a professor of TungHai University, Taiwan, the director of database and network security laboratory and chairperson of Department of Information management of the University. He is also a member of IEEE Computer Society and one of the editorial board members of at least 6 international journals.