Editorial
The 10th International Conference on Network and System Security (NSS 2016)

Kuo-Hui Yeh, Chunhua Su, Jiageng Chen, Nai-Wei Lo

While the attack systems have become more easy-to-use, sophisticated, and powerful, interest has greatly increased in the field of building more effective, intelligent, adaptive, active and high performance defense systems which are distributed and networked. The NSS series conferences cover research on all theoretical and practical aspects related to network and system security, such as authentication, access control, availability, integrity, privacy, confidentiality, dependability and sustainability of computer networks and systems. The 10th International Conference on Network and System Security (NSS 2016) was held in Taipei, Taiwan on 28-30 September, 2016. The aim of NSS 2016 is to provide a leading edge forum to foster interaction between researchers and developers with the network and system security communities, and to give attendees an opportunity to interact with experts in academia, industry, and governments. More information about the conference can be found at its website http://nsclab.org/nss2016. The main goal of this special issue is to publish outstanding studies from NSS 2016. After a rigorous peer review process, we selected 3 high-quality papers from NSS 2016.

The first article, entitled "Efficient and Publicly Verifiable Outsourcing of Large-Scale Matrix Multiplication" is presented by Sheng et al.. In this study, the issue of publicly verifiable matrix multiplication is investigated. The authors pointed out that the existing schemes are inefficient in practice due to the utilization of computationally expensive operations during public verification. They thus introduced a one-dimensional vector-based verification procedure to reduce the complexity, i.e. from $O(n^2)$ to $O(n)$, which is inverted from the original two-dimensional matrix. In addition, a fast algorithm, for the computation of batch of exponentiations, is proposed to pursue better efficiency. The second article, entitled "An Anti-Shoulder-surfing Authentication Scheme of Mobile Device," is proposed by Luo et al.. In this research, an authentication mechanism, enabling users to send out misleading information to attackers, was introduced to conquer shoulder-surfing problem. The misleading information consists of user's pressure values measured by smartphone touchscreens. In a normal authentication process, the systems detected each pressure value entered by the users and determined whether it was a true password or a misleading information. The resistance to shoulder-surfing attack is thus guaranteed because the attacker is unable to differentiate between true password and misleading information. The third article entitled, "A Proxy Transitive Signature Scheme," is proposed by Zhu et al.. The authors presented a digital signature scheme, integrating the concepts of proxy signature and transitive signature, for privacy preservation in graph-based big data systems. The scheme guarantees the signer to authenticate a graph in a cost-saving manner. Additionally, the proposed scheme is provably secure under the random oracle model with the DL and one-more BDH assumptions.

Acknowledgments

We would like to sincerely thank all the authors and reviewers for the tremendous efforts towards the success of this special issue.

Guest Editors

Kuo-Hui Yeh is an Associate Professor with the Department of Information Management, National Dong Hwa University, Hualien, Taiwan. He received M.S. and Ph.D. degrees in Information Management from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2005 and 2010, respectively. Dr. Yeh has authored over 90 articles in international journals and conference proceedings. His research interests include IoT security, Blockchain, mobile security, NFC/RFID security, authentication, digital signature, data privacy and network security. He is currently an Editor of IEEE Access, Journal of Internet Technology (JIT), Security and Communication Networks (SCN) and Data in Brief, and has served as a guest editor for Future Generation Computer Systems (FGCS), International Journal of Information Security (IJIS), JIT, Sensors and Cryptography. In addition, Dr. Yeh has participated in the organization committee of DSC 2018, SPCPS 2017, NSS 2016, RFIDsec'14 Asia and RFIDsec'12 Asia,

*Corresponding Author: Kuo-Hui Yeh; E-mail: khyeh@gms.ndhu.edu.tw

and he has served as a TPC member of 26 international conferences/workshops on information security. He is a Senior Member of the IEEE.

Chunhua Su is an Associate Professor of University of Aizu, Japan. He joined Osaka University from April 2016 to March 2017 as an Assistant Professor. He has worked as a research scientist in the Cryptography & Security Department of the Institute for Infocomm Research, Singapore from 2011-2013. From 2013-2016, he has worked as an Assistant Professor in Japan Advanced Institute of Science and Technology. His research interests include cryptographic protocols, privacy-preserving technologies and IoT security & privacy.

Jiageng Chen received the B.S. degree from the School of Computer Science and Technology, Huazhong University of Science and Technology (HUST) in 2004 and received his M.S. and PhD of computer science from the School of Information Science, Japan Advanced Institute of Science and Technology (JAIST) in 2007 and 2012, respectively. He was working as an Assistant Professor in School of Information Science, Japan Advanced Institute of Science and Technology from 2012 to 2015. And currently, he is an Associate Professor at the School of Computer, Central China Normal University. He is the Associate Editor of Journal of Information Security and Application, and he has served as a guest editor for Future Generation Computer Systems and Wireless Communications and Mobile Computing. His research areas include cryptography, especially in the areas of algorithms, cryptanalysis, data analysis, secure designs and so on.

Nai-Wei Lo received the B.S. degree in engineering science from National Cheng Kung University, Tainan, Taiwan, in 1988 and the M.S. and Ph.D. degrees in computer science and electrical engineering from the State University of New York at Stony Brook, Stony Brook, NY, USA, in 1992 and 1998, respectively. He is currently a Professor with the Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, and the Director of Taiwan Information Security Center, National Taiwan University of Science and Technology (TWISC@NTUST). His research interests include application and system security, IoT/IoV security, cloud security and Web technology. He currently serves as an associate editor of Journal of Information Security and Applications. He is a senior member of the IEEE.