

Guest Editorial: Security and Privacy for Contemporary Network Computing Environment

Joonsang Baek*, Willy Susilo, and Jongkil Kim

Institutue of Cybersecurity and Cryptology, University of Wollongong, Australia

Published: March 31, 2019

In network computing, computers and devices are not stand-alone but intimately linked together to perform various tasks and share resources. Network computing has become more and more sophisticated through technologies such as network virtualization, where hardware networks can be logically partitioned, and cloud computing, where the network resources are stored, managed and processed in the servers located remotely. Other mobile network technologies which integrate various devices into our networking systems have made the network computing environment more versatile. However, the sophistication and versatility added to the current network computing environment have inevitably caused many security and privacy issues to arise. In this special issue, five group of authors investigate these issues and suggest their solutions. We note that the first two papers in this issue [1, 2] are full versions of the papers presented at the 12th International Conference on Provable Security (ProvSec' 18), Jeju Island, Korea, 25-28 October 2018.

The first paper [1], *Towards Modeling Privacy in WiFi Fingerprinting Indoor Localization and its Application*, focuses on privacy models for privacy-preserving WiFi fingerprint based indoor localization (PPIL) schemes. In order to cover the state-of-the-art practical attacks, this paper proposes the first formal security model that formulates the security goals of both client-side and server-side privacy beyond the curious-but-honest setting. In particular, the proposed model considers various malicious behaviors such as exposing secrets of principles, choosing malicious WiFi fingerprints in location queries and specifying the location area of a target client.

The second paper [2], *BAdASS: Preserving Privacy in Behavioural Advertising with Applied Secret Sharing*, presents “BAdASS”, a novel privacy-preserving protocol for Online Behavioural Advertising that achieves significant performance improvements over the state-of-the-art without disclosing any information about users’ interests to any party. BAdASS ensures user privacy by processing data within the secret-shared domain, using the heavily fragmented shape of the online advertising landscape to its advantage and combining efficient secret-sharing techniques with a machine learning method commonly encountered in existing advertising systems.

The third paper [3], *Multi-View Permission Risk Notification for Smartphone System*, investigates how privacy notification interface can play an important role in assisting users in making informed decision regarding permission control. To address this issue, the paper proposes a multi-view privacy notification mechanism that provides customized notification interfaces that help users obtain necessary information about the risk behind granting a permission. The implementation of the proposed model

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications(JoWUA), 10:1 (Mar. 2019), pp. 1-3
DOI: 10.22667/JOWUA.2019.03.31.001

*Lead Guest Editor: School of Computing and Information Technology, University of Wollongong, Northfields Ave, Wollongong NSW 2522, Australia. Web:<https://www.uow.edu.au/~baek>

includes a new design of User Interface (UI), interpreting apps' activities risks and users' preferences adaption.

The fourth paper [4], *An Analytical Approach to Using and Implementing Beacons: Opportunities and Challenges*, explores the advantages, disadvantages and challenges of using and implementing beacon technology by qualitatively analyzing reliable articles, reports and applications as well as 50 software applications ("Apps") that operate on iOS and Android platforms. The research aims to provide a clear insight into beacon technology and the opportunities it offers to improve user experiences on mobile devices. The findings indicate that beacons' interaction with mobile applications enhances users' experience and satisfaction by enabling indoor navigation and proximity navigation. However, the paper also discusses several challenges such as privacy, security and applications' usability issues.

The last paper [5], *On the Security of a Privacy-Preserving Ranked Multi-Keyword Search Scheme*, studies the ranked keyword search over encrypted cloud data and presents cryptanalysis on the privacy-preserving ranked multi-keyword search scheme, which was proposed by Zhang et al.

We sincerely appreciate the hard work the authors have put in for their papers. We are also grateful to all the reviewers for their time and efforts to carefully review the papers and for the suggestions to improve the quality. Finally, our special thanks go to Prof. Ilsun You, Editor in Chief of the JoWUA, for his timely support for preparing this special issue.

Joonsang Baek, Willy Susilo, and Jongkil Kim
Guest Editors
March 2019

References

- [1] Z. Yang and K. Järvinen, "Towards Modeling Privacy in WiFi Fingerprinting Indoor Localization and its Application," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 10, no. 1, pp. 4–22, March 2019.
 - [2] L. J. Helsloot, G. Tillem, and Z. Erkin, "BADASS: Preserving Privacy in Behavioural Advertising with Applied Secret Sharing," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 10, no. 1, pp. 23–41, March 2019.
 - [3] C. Fung, B. Rashidi, and V. G. Motti, "Multi-View Permission Risk Notification for Smartphone System," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 10, no. 1, pp. 42–57, March 2019.
 - [4] H. K. Almathami, M. A. Alrafiee, E. Vlahu-Gjorgievska, and K. T. Win, "An Analytical Approach to Using and Implementing Beacons: Opportunities and Challenges," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 10, no. 1, pp. 58–74, March 2019.
 - [5] M. Noroozi, Z. Eslami, and J. Baek, "On the Security of a Privacy-Preserving Ranked Multi-Keyword Search Scheme," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 10, no. 1, pp. 75–85, March 2019.
-

Author Biography



Joonsang Baek is a Senior Lecturer in the School of Computer Science and Information Technology and a member of the Institute of Cybersecurity and Cryptology, University of Wollongong (UOW), Australia. He was a Research Scientist in the Institute for Infocomm Research, Singapore, and an Assistant Professor in the Khalifa University of Science and Technology, United Arab Emirates. Joonsang received his PhD from Monash University, Australia, in 2004. His PhD thesis was on security analysis of signcryption, and has received great attention from the research community. He has published his work in numerous reputable journals and conference proceedings. His current research interests are in the field of applied cryptography and cybersecurity. He has also served as a Program Committee Member and the Chair for a number of renowned conferences on information security and cryptography.



Willy Susilo is a Senior Professor in the School of Computing and Information Technology, Faculty of Engineering and Information Sciences in University of Wollongong, Australia. He is the director of Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong. Willy is an innovative educator and researcher. Currently, he is the Head of School of Computing and Information Technology at UOW (2015 - now). Prior to this role, he was awarded the prestigious Australian Research Council Future Fellowship in 2009. He was the former Head of School of Computer Science and Software Engineering (2009 - 2010) and the Deputy Director of ICT Research Institute at UOW (2006 - 2008). He is the Editor in Chief of the Information journal. Willy obtained his PhD from the University of Wollongong in 2001. He has published more than 300 papers in journals and conference proceedings in cryptography and network security. He has served as the program committee member of several international conferences. In 2016, he was awarded the "Researcher of the Year" at UOW, due to his research excellence and contributions. His work on the creation of short signature schemes has been well cited and it is part of the IETF draft.



Jongkil Kim Jongkil Kim received his PhD in Computer Science from the University of Wollongong (UOW), Wollongong, Australia in 2016. He is currently a Lecturer in the School of Computing and Information Technology and a member of Institute of Cybersecurity and Cryptology in UOW. His main research interest is in functional encryption and network security. He has authored multiple publications in an information security area.