Date of current version August 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2855258

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: SECURITY AND PRIVACY IN APPLICATIONS AND SERVICES FOR FUTURE INTERNET OF THINGS

The Internet of Things (IoT) has emerged as an important field of future network research that focuses on ubiquitous service patterns and universal access for people, devices, processes, etc. Motivated by great market demand and potential profit, future innovations for the application and accommodation for IoT will soon be realized and deployed expeditiously. However, those innovations will inevitably expose IoTs to security and privacy risks. Our society has witnessed tremendous concerns about these issues. Therefore, examining IoT applications and services closely for security and privacy vulnerabilities is of the utmost importance and can be further realized in three dimensions, namely, network architectural principles, application design, and high quality of service. From small atomic elements of the network to entire service packages, fine-grained verification should be performed to reduce security and privacy risks of an individual or the entire network.

In this Special Section of IEEE *Access*, researchers from various fields of study in relation to IoT have contributed their high-quality articles, further advancing the understanding of security and privacy issues of applications and services for the future Internet of Things. IEEE journals are considered the flagships in the engineering field. Among them, IEEE *Access* is gaining huge popularity because of its open access publications. This Special Section received tremendous support from authors all across the world and the number of submissions was high. After a rigorous peer review, 12 articles have been published under this Special Section topic.

Considering the demand for future IoT, online reviews have been a huge source of information gathering and they help organizations to improve their functionalities and offer a wide range of services. However, fake opinions and falsification of reviews have caused negative impacts on such services. In the article by *Rout et al.* (Revisiting semi-supervised learning for online deceptive review detection), the authors explain how semi-supervised learning methods can be used for detecting spam reviews, and demonstrated its utility using a data set of a hotel review system. IoT networks are facilitated through the use of Software Defined Networks (SDNs), which help fixate the QoS through their centralized and programmable management. Due to the limited resources in both the data plane and the control plane, SDN is vulnerable to the new-flow attack, which can disable the SDN-based IoT by exhausting the switches or the controller with numerous false requests. Such an issue is resolved by *Xu et al.* (Defending against new-flow attack in SDN-based Internet of Things) by using a smart security mechanism.

Another major advantage of IoT is a smart city formation. Dynamic nodes such as drones efficiently accommodate many services for users. However, their security is extremely tedious and to resolve this, *Won et al.* (Certificateless cryptographic protocols for efficient drone-based smart city applications) proposed a certificate-less cryptographic protocol. The author extended their approach to a smart parking system while securing applications for drone-enabled smart cities.

Code Obfuscation can further enhance the security of IoT devices and can ensure privacy while preventing attackers from gaining the knowledge of program instances. To achieve this, *Cho et al.* (Security assessment of code obfuscation based on dynamic monitoring in android things) proposed a scheme that can quantitatively evaluate the level of hiding of APIs, which represent the function of the Android application based on machine learning theory. Constant key sizes will enable fast encryption for securing mobile-based IoT devices. Odelu *et al.* (Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts) proposed a new RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC) that operates with $O(1)$ time complexity for each decryption and encryption. The approach is efficient and suits well to the power-constraint devices.

In addition to satisfying security requirements, having light-weight authentication can further improve the delivery of low-powered devices. While highlighting the flaws of an existing approach, Jiang*et al*. (Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks) proposed a lightweight and secure user authentication protocol based on the Rabin cryptosystem, which has the characteristic of computational asymmetry. ProVerif was used to demonstrate that the proposed scheme fulfills the required security properties. In another solution, Lu *et al.* (A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT), proposed a lightweight privacy-preserving

data aggregation scheme, called Lightweight Privacy-preserving Data Aggregation, for fog computing-enhanced IoT. Detailed security analyses, especially the enhanced differential privacy analyses, show that the proposed approach is secure under the defined security model.

Risk assessment through model checking can prevent IoT devices from different kind of threats. In an approach by Mohsin et al. (IoTRiskAnalyzer: A probabilistic model checking based framework for formal risk analytics of the Internet of Things), the authors proposed the IoTRiskAnalyzer framework for formally and quantitatively analyzing the security risks using probabilistic model checking. IoTRiskAnalyzer takes vulnerability scores, candidate IoT configurations, and attacker's capabilities as inputs for evaluations. This tool is automated for prioritizing the inputs.

While securing the transmissions in IoT enables applications, route optimization is one of the crucial challenges. For this Shin et al. (Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks) proposed a novel security protocol using the Diffie-Hellman algorithm. The proposed protocol is efficient in securing transmission of smart home IoT networks while preventing any overheads in the system. The protocol is verified through a popular BAN logic technique and AVISPA tool.

Traditional secure key storage is computationally expensive, and hence a novel solution is required for securing the IoT applications and devices. Huth et al. (Securing Systems with Indispensable Entropy: LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things) considered this requirement and proposed construction of a device-server authentication system providing outsider chosen perturbation security and pre-application robustness. The authors demonstrated that this implementation can be performed by using only 1.45 KB of SRAM and 9.8 KB of Flash memory on an 8-bit microcontroller.

As the devices in IoT have limited battery life, access management and control should be attained through a low-complex solution. Access control is one of the most important aspects of security and privacy in IoT networks. Uriarte et al. (Expressive Policy-Based Access Control for Resource-Constrained Devices) proposed an access control model that uses a policy language for dynamic fine-grained policy enforcement in the sensors based on local context conditions. The authors also proposed a novel security protocol, termed as Hidra and analyzed its feasibility for access management.

Finally, a survey (Robustness, security and privacy in location-based services for future IoT: A survey) that covers an in-depth evaluation of threats for future IoT networks is presented by Chen et al. The authors elaborated in detail on the security and privacy threats that are related to positioning of devices in future IoT. The authors also discuss the state-of-the-art of policy regulations regarding security of positioning solutions and legal instruments to location data privacy.

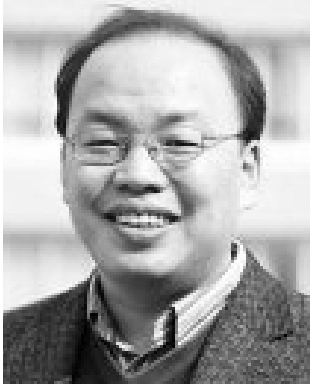
We are happy with the technical depth, reach, and diversification of this Special Section, and also hope that it will further advance the technical community's understanding of security and privacy of issues in applications and services for the Future Internet of Things. Finally, we want to extend our sincere gratitude to all the authors and reviewers for the tremendous efforts, and the Editor-in-Chief and Staff Members for their timely support and guidance.

ILSUN YOU, *Guest Editor*
Soonchunhyang University
Asan, South Korea

CAROL FUNG, *Guest Editor*
Virginia Commonwealth University
Richmond, VA 23284 USA

JOONSANG BAEK, *Guest Editor*
University of Wollongong
Wollongong, NSW 2522, Australia

VICTOR C. M. LEUNG, *Guest Editor*
The University of British Columbia
Vancouver, BC V6T 1Z4, Canada



ILSUN YOU (SM'13) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was with THIN multimedia, Inc., Internet Security, and Hanjo Engineering Co., Ltd., as a Research Engineer. He is currently an Associate Professor with the Information Security Engineering Department, Soonchunhyang University. He serves as the EiC for the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* and as an Associate Editor for *Information Sciences*, the *Journal of Network and Computer Applications*, the IEEE Access, *Intelligent Automation and Soft Computing*, the *International Journal of Ad Hoc and Ubiquitous Computing*, *Computing and Informatics*, and the *Journal of High Speed Networks*. His main research interests include internet security, authentication, access control, and formal security analysis. He is a Fellow of the IET.

CAROL FUNG received the bachelor's and master's degrees in computer science from the University of Manitoba, Canada, and the Ph.D. degree in computer science from the University of Waterloo, Canada. She has been a Visiting Scholar with POSTECH, South Korea, a Software Engineer Intern with Google, and a Research Intern with BlackBerry. Her research interests include collaborative intrusion detection networks, social networks, security issues in mobile networks and medical systems, location-based services for mobile phones, and machine learning in intrusion detection. She was a recipient of the Young Professional Award in the IEEE/IFIP IM 2015, the Alumni Gold Medal of the University of Waterloo in 2013, the Best Dissertation Awards in IM2013, the Best Student Paper Award in CNSM2011, the Best Paper Award in IM2009, and numerous prestigious awards and scholarships including the Google Anita Borg Scholarship, the NSERC Post-Doctoral Fellowship, the David Cheriton Scholarship, the NSERC Postgraduate Scholarship, and the President's Graduate Scholarship.

JOONSANG BAEK received the Ph.D. degree from Monash University, Australia, in 2004. His Ph.D. thesis was on security analysis of signcryption, and has received great attention from the research community. He was a Research Scientist with the Institute for Infocomm Research, Singapore, and an Assistant Professor with the Khalifa University of Science and Technology, United Arab Emirates. He is currently a Senior Lecturer with the School of Computer Science and Information Technology, University of Wollongong, Australia. 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.

VICTOR C. M. LEUNG (S'75–M'89–SM'97–F'03) is currently a Professor of electrical and computer engineering and the holder of the TELUS Mobility Research Chair with The University of British Columbia (UBC). He has co-authored over 1100 technical papers in archival journals and refereed conference proceedings, several of which had won best paper awards. His research is in the broad areas of wireless networks and mobile systems. He was a recipient of the IEEE Vancouver Section Centennial Award, the 2012 UBC Killam Research Prize, and the 2017 Canadian Award for Telecommunications Research. He co-authored papers that won the 2017 IEEE ComSoc Fred W. Ellersick Prize and the 2017 IEEE Systems Journal Best Paper Award. He is a fellow of the Royal Society of Canada, the Canadian Academy of Engineering, and the Engineering Institute of Canada. He serves on the editorial boards of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, the IEEE TRANSACTIONS ON CLOUD COMPUTING, the IEEE ACCESS, and several other journals.