Digital Communications and Networks 7 (2021) 245–246

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Editorial for special issue on ”security and privacy protection in the era of IoT devices”

IoT devices like smartphones have become an important personal assistant and an indispensable part of our daily life and work. As more and more users storing their private data on their mobile phones, it becomes imperative to develop secure mobile operating systems, secure mobile clouds and applications, and secure mobile devices. In recent years, IoT device security, like smartphone security, depends not only on the phones, but also on the mobile device management technology that controls and manages device security. As a result, there is an increasing need for security solutions to protect users' sensitive and private information in the IoT environment. This special issue focuses on security and privacy issues on IoT devices and identifies new schemes and mechanisms for constructing a safe and robust IoT environment.

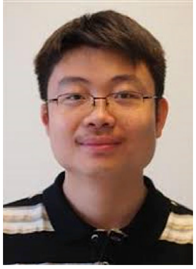
In the first paper entitled “Secure K-Nearest Neighbor Queries in Two-tiered Mobile Wireless Sensor Networks”, Fan et al. focused on the secure KNN query technology in TMWSNs and proposed two secure KNN query algorithms in TMWSNs named BAFSKQ (the basic algorithm of KNN query) and SEKQAM (the KNN query algorithm based on MR-Tree), respectively. They then theoretically analyzed the security of these two KNN query methods, and it is proved that they can effectively ensure the privacy of the information on the storage nodes and have good soundness and integrity. In the evaluation, they found that SEKQAM has a lower communication cost than BAFSKQ in most cases.

In the second paper entitled “Challenge-based Collaborative Intrusion Detection in Software-Defined Networking: An Evaluation”, Li et al. focused on challenge-based Collaborative Intrusion Detection Networks (CIDNs) and evaluated its performance in Software Defined Networking (SDN). For challenge-based CIDNs, since the testing node knows the actual severity in advance, the satisfaction level can be calculated based on the feedback received. The experimental results indicate that such a detection mechanism could work well in SDN by identifying malicious nodes quickly.

In the third paper entitled “User location privacy protection mechanism for location-based services”, He and Chen pointed out that protecting users' location privacy has become an important issue for the current Location-Based Services (LBS). They built a robust authentication mechanism through the critical negotiation phase to ensure the system's overall authentication security. They then designed a user location privacy protection mechanism that is suitable for the LBS based on the privacy proximity test problem. This method guarantees the trust between the users and the service providers under a strong authentication mechanism while ensuring users' privacy.

In the fourth paper titled “Substring-searchable attribute-based encryption and its application for IoT devices”, Sun et al. introduced an Attribute-Based Encryption (ABE) scheme called Sub-String Searchable ABE (SSS-ABE). Compared with the traditional ABE schemes, the SSS-ABE scheme can query the ciphertext, and the data user can know whether the ciphertext contains the desired content before downloading all the ciphertexts. This can reduce the communication overhead.

On the whole, the special issue papers cover a broad range of research on security and privacy issues on IoT devices and discuss various security threats and potential solutions. The team of guest editors would like to thank Editor-in-Chief Jinzhao Lin and Managing Editor Yi Guo for their tremendous support and the paper authors and the reviewers for their contributions.



Dr. Weizhi Meng is currently an Associate Professor in the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong. Before joining DTU, he worked as a research scientist in Institute for Infocomm Research, A*Star, Singapore. He won the Outstanding Academic Performance Award during his doctoral study and is a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in 2014 and 2017. His primary research interests are cybersecurity and intelligent technology in security, including intrusion detection, smartphone security, biometric authentication, HCI security, trust computing, blockchain in security, and IoT security. He served as program committee members for 50+ international conferences. He served as guest editor for FGCS, JISA, Sensors, CAEE, IJDSN, DCN, SCN, WCNC, etc.

https://doi.org/10.1016/j.dcan.2021.04.003

Dr. Daniel Xiapu Luo is an associate professor in the Department of Computing, The Hong Kong Polytechnic University. His current research interests include Blockchain Contracts, Mobile/IoT Security and Privacy, Network Security and Privacy, and Software Engineering. His work appeared in top venues of security, software engineering and networking, such as IEEE S&P/USENIX SEC/CCS/NDSS, ICSE/FSE/ASE/ISSTA, INFOCOM/SIGMETRICS, etc. He has received seven best paper awards (e.g., INFOCOM′18, ISPEC′17, ISSRE′16, etc.).

Dr. Chunhua Su received the B.S. degree from Beijing Electronic and Science Institute in 2003 and received his M.S. and PhD in computer science from the Faculty of Engineering, Kyushu University in2006 and 2009, respectively. He is currently working as a Senior Associate Professor in the Division of Computer Science, University of Aizu. He once worked as a postdoctoral fellow in Singapore Management University from 2009 to 2011 and a research scientist in the Cryptography & Security Department of the Institute for Infocomm Research, Singapore, from 2011 to 2013. From 2013 to 2016, he has worked as an Assistant professor in the School of Information Science, Japan Advanced Institute of Science and Technology. From 2016 to 2017, he worked as Assistant Professor in the Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in machine learning, IoT security, & privacy. He has published more than 100 papers in international journals and conferences.

Prof. Debiao He received his PhD degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, Wuhan, China, in 2009. He is currently a professor in the School of Cyber Science and Engineering, Wuhan University. He has published more than 150 research papers in international conferences and journals. His work has been cited more than 7000 times at Google Scholar. His main research interests include applied cryptography and information security. He serves as an editorial board member of several journals, such as *Computers & Electrical Engineering*, *Journal of Medical Systems*, *Journal of Information Security and Applications*, and *IET Wireless Sensor Systems*.

Dr. Marios Anagnostopoulos is an Assistant Professor in the Department of Electronic Systems, Aalborg University, and specifically in the Communication, Media and Information Technologies section. He is a member of the Cyber Security research group. He holds a B.Sc. in Computer Science from the Computer Science Department of University of Crete, Greece, and a Master's degree in Information and Communication Systems Security from the University of the Aegean, Greece. Furthermore, Marios holds a Ph.D. degree in Information and Communication Systems Engineering, also from the University of the Aegean. After that, he has worked as Post-Doctoral Research Fellow within cybersecurity at the Norwegian University of Science and Technology (NTNU) and the Singapore University of Technology and Design (SUTD). His research interests are in the fields of cybersecurity and privacy, and more specifically in DNS security, IoT security, and security education and awareness.

Dr. Qian Chen is an Assistant Professor with the Department of Electrical and Computer Engineering at the University of Texas at San Antonio (UTSA). Before joining UTSA, Dr. Chen was an Assistant Professor and Coordinator of the Computer Science Technology Program at Savannah State University. She received her PhD degree in Electrical and Computer Engineering from Mississippi State University in 2014. Her primary research area is autonomic computing and cybersecurity. Dr. Chen's current research involves autonomic security management for distributed systems, industrial control systems (e.g., SCADA), high-performance computing, and the Internet of Things (IoT) ecosystems (e.g., healthcare information systems, smart cities, etc.). Her research topics include risk assessment, attacks estimation, vulnerabilities investigation, intrusion detection and response and end-to-end security solution development. Her research projects were funded by the National Science Foundation, Department of Energy, Department of Homeland Security, Oak Ridge National Laboratory, Mississippi State University and Savannah State University.

Weizhi Meng*
Technical University of Denmark, Denmark

Daniel Xiapu Luo
Hong Kong Polytechnic University, China

Chunhua Su
University of Aizu, Japan

Debiao He
Wuhan University, China

Marios Anagnostopoulos
Aalborg University, Denmark

Qian Chen
University of Texas at San Antonio, USA

* Corresponding author.
E-mail address: weme@dtu.dk (W. Meng).