JCN October Special Issue on IoT Security and Privacy

Daji Qiao, Farid Nait-Abdesselam, Ryan Gerdes, Tie Qiu

The emerging IoT (Internet of Things) paradigm aims to connect all kinds of different physical objects together and make them accessible from the Internet, with advanced sensing, actuation, communications, and networking technologies. IoT systems vary in type, scale, and function. They range from Internet of Vehicles, to Industrial Internet of Things, to Internet of Battlefield Things and Internet of Medical Things. Gartner predicts that tens of billions of IoT devices will be in use in the near future. Many low-cost IoT devices have little processing power or storage capacity, resulting in poor built-in security capabilities. This allows these devices to be used as ingress points to access the broader IT or critical infrastructure. Because of the expanded attack surface, IoT security and privacy has become a pressing issue. Every threat against the IoT may constitute a more severe threat to the IT or critical infrastructure behind the IoT. Thus, it is imperative to study and understand the security and privacy risks related to IoT and to propose innovative solutions to deal with these risks.

This special issue received 16 submitted manuscripts, out of which 7 papers have been accepted for publication. The editors would like to thank the authors of all papers for their submissions and special thanks go to the reviewers for their help in allowing us to complete the reviews and decisions in a timely fashion. The papers in this special issue will report research advances in IoT Security and Privacy in the following two aspects: **Algorithms and Protocols**; **Systems and Applications**.

IoT Security and Privacy – Algorithms and Protocols: This section includes three papers that overview the IoT security and privacy research, and propose new security and privacy algorithms and protocols for IoT networks and wireless sensor networks in general. The first paper "On the Security Aspects of Internet of Things: A Systematic Literature Review" by *Evandro Macedo et al.* performs a systematic and comprehensive review on research in the following four security aspects of the IoT: authentication, access control, data protection, and trust, and then identifies open issues and challenges that provide a useful guidance for future research studies in this area. Next, the paper "Sentinel Based Malicious Relay Detection in Wireless IoT Networks" by *Anshoo Tandon et al.* designs an effective and practical scheme to protect wireless IoT networks from data integrity and selective forwarding attacks launched by malicious relays. Finally, the paper "Security Cooperation Model Based on Topology Control and Time Synchronization for Wireless Sensor Networks" by *Zhaobin Liu et al.* presents a security collaboration model between wireless sensor and IoT nodes, based on topology control and time synchronization.

IoT Security and Privacy – Systems and Applications: This section selects four papers that develop new security and privacy techniques for various practical IoT systems and applications. The first two papers discuss how UAVs (Unmanned Aerial Vehicles) may be used to enhance the security and privacy performance of an IoT system. In particular, the paper "UAV-enabled Friendly Jamming Scheme to Secure Industrial Internet of Things" by *Qubeijian Wang et al.* proposes to have multiple UAVs emit jamming signals in an intelligent manner, in order to disrupt eavesdropping activities on industrial IoT devices without affecting legitimate communications between these devices. The paper “BUAV: A Blockchain Based Secure UAV-Assisted Data Acquisition Scheme in Internet of Things” by *Anik Islam et al.* presents a secure data acquisition scheme to transfer data from IoT nodes to the MEC (Mobile Edge Computing) server, based on the blockchain technology and the assistance of a UAV. The next paper “An Intelligent Agriculture Network Security System Based on Private Blockchains” by *Hsin-Te Wu et al.* also applies the blockchain technology but for a different application, to prevent DDoS (Distributed Denial-of-Service) attacks against intelligent agriculture systems. Finally, the paper “Worth One Minute: An Anonymous Rewarding Platform for Crowd-Sensing Systems” by *Lorenz Klopfenstein et al.* studies how IoT devices and their users may participate in crowd-sourcing applications while preserving their anonymity, and a general-purpose rewarding system based on anonymous vouchers has been designed and implemented for this purpose.

Daji Qiao is currently an Associate Professor in the Department of Electrical and Computer Engineering at Iowa State University, Ames, Iowa, USA. He received his PhD degree in Electrical Engineering: Systems from The University of Michigan, Ann Arbor, Michigan in 2004. His research interests include sensor networks and Internet of Things (IoT), wireless networking and mobile computing, and cyber security. He has served on the organizing and technical program committees of many networking and communications conferences, such as IEEE INFOCOM, Globecom, WCNC, SECON, ICCCN, ICDCS, MASS, and WoWMoM. He is a senior member of the IEEE.

Farid Nait-Abdesselam is currently a Professor in the Department of Computer Science and Electrical Engineering at University of Missouri Kansas City, KCMO, USA. He received his PhD degree in Computer Science from University of Versailles, France, in 2000. His research interests include wireless and mobile networking, security, and networked healthcare systems. He has served on the organizing and technical program committees of many networking and communication conferences, such as IEEE ICC, GLOBECOM, WCNC, and LCN. He is the editor in chief of the International Journal of Network Science, and associate editor of many other journals, such as Wiley Security & Privacy. He is a senior member of the IEEE.

Ryan Gerdes is currently an Assistant Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech, Arlington, Virginia, USA. He received his PhD degree in Electrical Engineering from Iowa State University, Ames, Iowa in 2011. His research interests include cyber-physical systems security (physical-layer sensor/actuator spoofing and countermeasures, devising/countering attacks against control systems, and secure localization), physical layer identification (identifying devices based on electrical side-channels), and integrated circuit security (designing, detecting, and remotely triggering malicious logic). He has served on the organizing and technical program committees of many security conferences, such as IEEE CNS, ACSAC, DSN, and SecureComm. He is a member of the IEEE.

Tie Qiu is currently a Full Professor at School of Computer Science and Technology, Tianjin University, China. Prior to this position, he held assistant professor in 2008 and associate professor in 2013 at School of Software, Dalian University of Technology. He) received Ph.D degree in computer science from Dalian University of Technology in 2012. He was a visiting professor at electrical and computer engineering at Iowa State University in U.S. (2014-2015). He serves as an associate editor of IEEE Transactions on SMC: Systems, area editor of Ad Hoc Networks (Elsevier), associate editor of IEEE Access Journal, Computers and Electrical Engineering (Elsevier), Human-centric Computing and Information Sciences (Springer), a guest editor of Future Generation Computer Systems. He serves as General Chair, Program Chair, Workshop Chair, Publicity Chair, Publication Chair or TPC Member of a number of international conferences. He has authored/co-authored 9 books, over 130 scientific papers in international journals and conference proceedings, such as IEEE/ACM ToN, IEEE TMC, TKDE TII, TIP, TCY, TITS, TVT, IEEE Trans. SMC: Systems, IEEE Communications Surveys & Tutorials, IEEE Communications etc. There are 12 papers listed as ESI highly cited papers. He has contributed to the development of 3 copyrighted software systems and invented 14 patents. He is a senior member of China Computer Federation (CCF) and a senior member of the IEEE and the ACM.