information

MDPI

Editorial

Special Issue on Mobile Systems, Mobile Networks, and Mobile Cloud: Security, Privacy, and Digital Forensics

Lei Chen [1,*], Wenjia Li [2] and Rami J. Haddad [3]

[1] Department of Information Technology, College of Engineering and Information Technology, Georgia Southern University, P.O. Box 8150, Statesboro, GA 30458, USA

[2] Department of Computer Science, School of Engineering and Computing Sciences, New York Institute of Technology, 1855 Broadway, New York, NY 10023, USA; wli20@nyit.edu

[3] Department of Electrical Engineering, College of Engineering and Information Technology, Georgia Southern University, P.O. Box 8045, Statesboro, GA 30458, USA; rhaddad@georgiasouthern.edu

* Correspondence: Lchen@georgiasouthern.edu

Received: 14 August 2017; Accepted: 14 August 2017; Published: 15 August 2017

The use of smartphones and mobile devices has become an indispensable part of everyone's daily life and work. With critical personal information, such as financial and medical information, and critical work related data being processed on mobile systems, mobile networks, and mobile cloud, it is particularly important that the development and advancement of secure mobile operating systems, secure mobile cloud and applications, secure mobile devices and cellular networks would not fall behind the ever-growing smartphone usage. The scope of this special issue encompasses the security, privacy, and digital forensics of mobile systems, mobile networks, and mobile cloud, including but not limited to Android, iOS, and Windows Mobile operating systems, mobile devices, systems and applications, the modeling, design, and testing of mobile systems, networks, and cloud with security and privacy in mind, secure mobile methodologies and algorithms, secure mobile applications, as well as cellular networks.

The special issue has received 15 submissions, all of which went through a rigorous peer-review process. The editors have jointly evaluated all submissions and are pleased to include seven high quality ones in this special issue based on the review ratings and comments. These seven papers range over various mobile networks and technologies, including conventional mobile networks, Radio Frequency Identification (RFID), Near Field Communications (NFC), Wi-Fi, Android Mobile Systems, and 45 GHz Millimeter Wave transmission. Meanwhile, the research findings also cover a wide range of aspects of security, privacy, and digital forensics, including balance and trade-off between security and flexibility/efficient of network protocols, mobile device authentication, secure and private Wi-Fi connections, mobile gaming security, digital forensics, and human security awareness. Each of these seven papers is briefly introduced in the following paragraphs.

Opportunistic mobile networks (OppNets), which represent a form of ad hoc networks, have recently been gaining popularity due to their independence of any mobile infrastructure. Opportunistic message forwarding is established between nodes whenever they are in close vicinity to each other through a continuous contact probing process. The main drawback is that the contact probing is a highly energy-consuming process. Periodic contact probing with a specific duty cycle was previously proposed to address this problem. However, it degrades the network connectivity, delivery ratio, and increases transmission delays. In paper "Efficient Listening and Sleeping Scheduling Mechanism Based on Self-Similarity for Duty Cycle Opportunistic Mobile Networks" the authors Feng Zeng, Yueyue Dou, Zhigang Chen, and Hui Liu proposed an adaptive scheduling mechanism based on self-similarity, in which Linear Minimum Mean Square Error predictor is used to predict the future contact information. While not directly tied to security or privacy, their proposed and validated adaptive scheduling model reduces the energy consumption in OppNets while maintaining the network's performance and improving its viability.

The utilization of radio frequency identification (RFID) technologies to identify objects using radio frequencies has been significantly increasing in the last decade. Recently, a new class of protocols, referred to as radio frequency identification grouping-proof protocols, was proposed that can generate an evidence of the simultaneous existence of a group of tags. This type of protocols has a wide range of applications, one of which is the medical field. Even though the current grouping-proof protocols are very useful, they suffer from low grouping-proof efficiency and some security vulnerabilities. In paper "A Lightweight RFID Grouping-Proof Protocol Based on Parallel Mode and DHCP Mechanism", the authors Zhicai Shi, Xiaomei Zhang, and Yihan Wang proposed a lightweight RFID grouping-proof protocol utilizing parallel communication mode, DHCP, and a broadcast mechanism to effectively complete the grouping proof without leaking any secure information to the reader, hence improving the privacy and security of the RFID system. This research helps improve the performance, security, and privacy of RFID system applications.

In recent years, we have witnessed a rapid growth in the number of mobile and smart devices in the world. While mobile devices become an indispensable part of our daily lives, there has been increasing concern about their security and privacy. In particular, the traditional authentication methods—such as password, PIN, or touchscreen swipe pattern—suffer from various social engineering types of attacks, such as shoulder surfing. Therefore, it is desirable to leverage on other types of authentication methods to better secure mobile devices. In the paper titled "Protecting Touch: Authenticated App-to-Server Channels for Mobile Devices Using NFC Tags", authored by Fernando Kaway Carvalho Ota, Michael Roland, Michael Hölzl, René Mayrhofer, and Aleardo Manacero, different types of existing Near Field Communication (NFC) tags have been evaluated to use as tokens to establish authenticated secure sessions between smartphone apps and web services. Based on the initial evaluation, the authors propose a user-friendly and practical secure authentication mechanism for mobile apps, the Protecting Touch (PT) architectures.

Despite the fact that Wi-Fi networks have made our Internet access experience extremely convenient and ubiquitous, the wide deployment of Wi-Fi networks also makes it much easier to violate users' privacy. In the paper titled "Insecure Network, Unknown Connection: Understanding Wi-Fi Privacy Assumptions of Mobile Device Users", the authors Bram Bonné, Gustavo Rovelo, Peter Quax, and Wim Lamotte conduct a user study with 108 participants to find out to what extent the privacy stance of mobile device users corresponds with their actual behavior. More specifically, the authors first monitor Wi-Fi networks that the participants' devices connect to and the connections made by apps on these devices, for a period of 30 days. Afterwards, participants are surveyed about their awareness and privacy sensitiveness. Interpreting from the study results, the authors find that although a higher expertise in computer networks generally corresponds to more awareness about the connections made by apps, neither this expertise nor the actual privacy stance of the participant translates to better security habits.

Geolocation capabilities of mobile devices allow the creation of innovative mobile applications such as the Pokémon GO, which received more than 10 million downloads in the first week of release and over 100 million downloads by the end of its first month after debut. Despite its popularity, Pokémon GO is linked to many public safety issues, such as distraction to drivers and robberies. Recognizing the need for forensic investigators to be able to analyze the data of this mobile app, in paper "Pokémon GO Forensics: An Android Application Analysis", Joshua Sablatura and Umit Karabiyik present their research on identifying and acquiring the forensic artifacts associated with this app. A new application-specific analysis tool for extracting such artifacts has been introduced, exceeding the capabilities of the Cellebrite's UFED. Their research is valuable in addressing the digital forensics of a trending mobile application and potentially enhancing public safety.

Mobile 5G networks and technologies have received rapidly increasing attention in recent research. Higher frequency bands, such as the millimeter wave, are considered promising for boosting the capacity of 5G, the next generation cellular networks. In paper "The Diffraction Research of Cylindrical Block Effect Based on Indoor 45 GHz Millimeter Wave Measurements", the authors Xingrong Li, Yongqian Li, and Baogang Li proposed four kinds of block diffraction models to study the diffraction research of cylindrical block (such as human and many objects with similar shapes) effect on 45 GHz millimeter wave in the indoor environment. While not directly tied to security or privacy, their proposed models and validated simulation results help contribute to possibly enhancing the capacity of the next generation cellular networks.

Humans are the weakest link in the chain of security and privacy. In paper "Security Awareness of the Digital Natives", authors Vasileios Gkioulos, GauteWangen, Sokratis K. Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou present the results of their research survey performed across a multinational sample of digital natives with distinct backgrounds and levels of competence in terms of security. With the aim of identifying divergences in user behavior due to regional, educational, and other factors, their research highlights the significant influences on the behavior of digital natives, arising from user confidence, educational background, and parameters related to usability and accessibility. This research helps to justify the need for further study and emphasizes human factors in the security of the digital world.

Due to time constraints, this special issue has no intent of presenting a complete scope of recent research findings and advancements in the security, privacy, and digital forensics of mobile systems, networks, and cloud. Nonetheless, it is the editorial team's intent to bring to the audience the essence of selected innovative and original research ideas and progress for the purpose of inspiring future research in this fast growing area.

Acknowledgments: The guest editors would like to give our special thanks to all the authors for making contributions to this special issue. We are also thankful to the editors and assistants at MDPI for providing helpful and prompt support. Last but not least, the editorial team would also express our appreciation to the editors' affiliated departments and colleges at Georgia Southern University and New York Institute of Technology for their continuous support in faculty's scholarly research and professional services.

Conflicts of Interest: The authors declare no conflict of interest.