future internet

MDPI

Editorial

Security and Privacy in Wireless and Mobile Networks

Georgios Kambourakis [1,*], Felix Gomez Marmol [2] and Guojun Wang [3]

[1] Department of Information and Communication Systems Engineering, University of the Aegean, 83100 Karlovasi, Samos, Greece

[2] Department of Information and Communications Engineering, University of Murcia, 30100 Murcia, Spain; felixgm@um.es

[3] School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China; csgjwang@gzhu.edu.cn

* Correspondence: gkamb@aegean.gr; Tel.: +30-227-308-2256

Received: 6 February 2018; Accepted: 7 February 2018; Published: 9 February 2018

Currently, at the dawn of 5G networks, and the era of the Internet-of-Things, wireless and mobile networking is becoming increasingly ubiquitous. In this landscape, security and privacy turn into decisive factors. That is, the mobile and wireless ecosystem is an ideal playground for many perpetrators: (a) handheld devices are used for critical tasks, such as e-commerce, bank transactions, payments, application purchases, as well as social interaction; (b) such devices uniquely identify their users and store sensitive and detailed information about them; and (c) despite all their sophistication, native security mechanisms of mobile operating systems can be bypassed, and several wireless interfaces and protocols have been proven to be vulnerable to attack. As the attacker is given so many alternative entry points for penetration, the creation of assaults against the end-user and the underlying systems and services have been augmented, both in amount, as well as in matters of complexity. It is, therefore, imperative that new and advanced security and privacy-preserving measures are deployed.

To cope with the aforementioned challenges, this special issue has been dedicated to the security and privacy aspects of mobile networks, wireless communications, and their apps. Particularly, apart from network and link layer security, the focus is on the security and privacy of mobile software platforms and the increasingly differing spectrum of mobile or wireless apps. Via both invited and open call submissions, a total of nineteen papers were submitted and nine have been finally accepted. Each manuscript underwent a rigorous review process involving a minimum of three reviews. All the accepted articles constitute original research work addressing a variety of topics pertaining to the above-mentioned challenges.

The first article by Wenjuan Li, Weizhi Meng and Lam For Kwok [1], focuses on collaborative intrusion detection networks (CIDN), which allow intrusion detection system nodes to exchange data with each other. The authors deal with insider attacks which typically are more difficult to identify. Particularly, by examining challenge-based CIDNs, they analyze the influence of advanced on-off attacks, where the attacker responds truthfully to one IDS node but behaves maliciously to another. The authors report results from two experiments using both simulated and real CIDN environments.

The work by Rezvan Almas Shehni, Karim Faez, Farshad Eshghi and Manoochehr Kelarestaghi [2], copes with Sybil types of attacks in mobile Wireless Sensor Networks (WSN), and proposes a computationally lightweight watchdog-based algorithm for detecting it. According to the authors' algorithm, the watchdog nodes collect detection information, which is then passed to a designated node for processing and identifying Sybil nodes. The highlights of their algorithm are the low communication overhead, and a fair balance between true and false detection rates. These qualities are proved via simulation and comparison against recent watchdog-based Sybil detection algorithms.

End-user privacy protection in smart home applications is the topic of the article contributed by Jingsha He, Qi Xiao, Peng He, and Muhammad Salman Pathan [3]. Given that attacks do not necessarily need access to the cipher, but can be mounted by simply analyzing the frequency of radio signals or the timestamp series, the authors argue that legacy encryption methods cannot satisfy the needs of privacy protection in such applications. Therefore, the daily activities of the people living in a smart home are at stake. To obfuscate the patterns of daily routines of smart home residents, they propose an adaptive method based on sample data analysis and supervised learning, which allows them to cope with fingerprint and timing-based snooping types of attacks. Via experimentation, the authors demonstrate that their method supersedes similar proposals in terms of energy consumption, latency, adaptability, and degree of privacy protection.

Radio Frequency Identification (RFID) systems are inherently prone to attacks because of the wireless nature of the communication channel between the reader and a tag. To protect the privacy of tags, the work by Zhibin Zhou, Pin Liu, Qin Liu and Guojun Wang [4] investigates ways of ensuring the tag's information security and providing guarantees that the system generates reliable grouping-proof. The authors note that since the verification of grouping-proof is typically done by the verifier, the reader is able to submit bogus proof data in the event of Deny of Proof attack. To remedy this issue, they propose an ECC -based, off-line anonymous grouping-proof protocol, which authorizes the reader to examine the validity of grouping-proof without being aware of the identities of tags. The protocol is examined in terms of both security and performance, showing that it can resist impersonation and replay attacks against the tags.

In the mobile app ecosystem, Pierpaolo Loreti, Lorenzo Bracciale and Alberto Caponi [5] stress that push notifications may lead to loss of end-user privacy. For instance, social networking apps use such notifications extensively (e.g., friendship request, tagging, etc.) via real-time channels. However, even in cases where the confidentiality of the channel is preserved, action anonymity may fail. That is because the actions that trigger a notification and the reception of the corresponding message can be uniquely correlated. They pinpoint that even when pseudonyms are in play, this situation can be exploited by attackers to reveal the real identity of the user of a mobile device. The authors call this situation a "push notification attack", and demonstrate that it can be exercised in an online or offline fashion.

The work by Stylianos S. Mamais and George Theodorakopoulos [6] deals with Online Behavioural Advertising (OBA). Concentrating on security, privacy, targeting effectiveness, and practicality, they categorize the available ad-distribution methods and identify their shortcomings. Based on opportunistic networking, they also propose a novel system for distributing targeted adverts in a social network. The highlights of this system are that it does not require trust among the users, and it is low in memory and bandwidth overhead. Moreover, their system blocks evil-doers from launching impersonation attacks and altering the ads with the intention of spreading malicious content. The same authors in [7] note that ad-Networks and publishers service commissions can be forged by non-human actors via the injection of fictitious traffic on digital platforms. This situation leads to financial fraud. Using opportunistic networking and a blockchain technology, they proposed an advert reporting system which is capable of identifying authentic Ad-Reports, i.e., those created by honest users. This is decided by examining, in a privacy-preserving way, the user's patterns when accessing adverts on their mobile device.

The security risks due to design shortcomings and vulnerabilities related to end-user behavior when interacting with mobile devices is the focus of the work by Vasileios Gkioulos, Gaute Wangen and Sokratis K. Katsikas [8]. They present the results of a survey conducted across a multinational sample of security professionals and compare them against those derived from their earlier study over the security awareness of digital natives (young people, born in the digital era). This has been done in an effort to identify differences between the conceptual user-models that security experts utilize in their professional tasks and user behavior. The main result is that, while influences from personal perceptions and randomness are not insignificant, the experts' understanding of the user behaviour does not follow a firm user-model.

The article by Andrea Guazzini, Ayca Sarac, Camillo Donati, Annalisa Nardi, Daniele Vilone and Patrizia Meringolo [9] it built around a very interesting observation: the ICT revolution changes our world and is having a crucial role as a mediating factor for social movements and political decisions. Moreover, the perception of this new environment (social engagement, privacy perception, sense of belonging to a community) may differ even in similar cultures. Motivated by the changes that have occurred due to the introduction of the web, the authors explore via a questionnaire instrument the inter-relations between the constructs of sense of community, participation and privacy compared with culture and gender. Their study took into account 180 participants from Turkey and Italy, with the aim to highlight the cultural differences in the perception of the aforementioned constructs. The analysis of results takes into consideration the recent history of both countries in terms of the adoption of new technologies, political actions, and protest movements.

Author Contributions: All authors contributed equally to this editorial.

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

References

1. Li, W.; Meng, W.; Kwok, L.F. Investigating the Influence of Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks. *Futur. Internet* **2018**, *10*, 6, doi:10.3390/fi10010006.
2. Almas Shehni, R.; Faez, K.; Eshghi, F.; Kelarestaghi, M. A New Lightweight Watchdog-Based Algorithm for Detecting Sybil Nodes in Mobile WSNs. *Futur. Internet* **2018**, *10*, 1, doi:10.3390/fi10010001.
3. He, J.; Xiao, Q.; He, P.; Pathan, M.S. An Adaptive Privacy Protection Method for Smart Home Environments Using Supervised Learning. *Futur. Internet* **2017**, *9*, 7, doi:10.3390/fi9010007.
4. Zhou, Z.; Liu, P.; Liu, Q.; Wang, G. An Anonymous Offline RFID Grouping-Proof Protocol. *Futur. Internet* **2018**, *10*, 2, doi:10.3390/fi10010002.
5. Loreti, P.; Bracciale, L.; Caponi, A. Push Attack: Binding Virtual and Real Identities Using Mobile Push Notifications. *Futur. Internet* **2018**, *10*, 13, doi:10.3390/fi10020013.
6. Mamais, S.S.; Theodorakopoulos, G. Private and Secure Distribution of Targeted Advertisements to Mobile Phones. *Futur. Internet* **2017**, *9*, 16, doi:10.3390/fi9020016.
7. Mamais, S.S.; Theodorakopoulos, G. Behavioural Verification: Preventing Report Fraud in Decentralized Advert Distribution Systems. *Futur. Internet* **2017**, *9*, 88, doi:10.3390/fi9040088.
8. Gkioulos, V.; Wangen, G.; Katsikas, S.K. User Modelling Validation over the Security Awareness of Digital Natives. *Futur. Internet* **2017**, *9*, 32, doi:10.3390/fi9030032.
9. Guazzini, A.; Sarac, A.; Donati, C.; Nardi, A.; Vilone, D.; Meringolo, P. Participation and Privacy Perception in Virtual Environments: The Role of Sense of Community, Culture and Gender between Italian and Turkish. *Futur. Internet* **2017**, *9*, 11, doi:10.3390/fi9020011.