Hindawi
Security and Communication Networks
Volume 2018, Article ID 5346596, 2 pages
https://doi.org/10.1155/2018/5346596

Editorial

Security and Privacy for Smart, Connected, and Mobile IoT Devices and Platforms

Karl Andersson,[1] **Ilsun You**,[2] **and Francesco Palmieri**[3]

[1]*Luleå University of Technology, Skellefteå, Sweden*
[2]*Soonchunhyang University, Chungcheongnam-do, Republic of Korea*
[3]*University of Salerno, Fisciano (SA), Italy*

Correspondence should be addressed to Karl Andersson; karl.andersson@ltu.se

Received 3 September 2018; Accepted 3 September 2018; Published 27 September 2018

1. Introduction

In recent years, with the rapid development of the smart city paradigm, the Internet of Things (IoT) has raised widespread concern in the whole ICT community. IoT refers to linking the sensors, controllers, machines, people, and things together by using local or wide area communication and cloud technologies, with the Internet as the glue, through a new way to build an intelligent things-to-things network. However, in the near future, the large-scale deployment of the IoT also needs to face many challenges, especially in security and privacy issues for smart, connected, and mobile IoT devices and platforms due to the fact that IoT has different characteristics from traditional communication networks, related to its specific features and threats. In particular, the security solutions for IoT must provide IoT nodes (things, users, servers, and objects) with data authenticity, confidentiality, integrity and freshness certification, and authorization. In addition, privacy protection must also be considered. Many IoT services and applications may expose sensitive and personal information which may be abused by attackers. The concept of privacy may be different, but it should protect the user's personal identity information and maintain a certain degree of anonymity, nonlinkability, and data confidentiality. Of course, it is also necessary to strike a balance between the availability and the security and privacy protection for IoT.

This special issue focuses on the IoT devices and platforms with respect to security and privacy preserving technologies for speeding up the technological progress and attracting more researchers' concerns about the development in this field. In addition, this special issue includes extended versions of the best papers presented at the 2nd International Symposium on Mobile Internet Security (MobiSec'17) held on Jeju, Jeju Island, Republic of Korea, on October 19–22, 2017.

For the current issue, we are pleased to introduce a collection of papers covering a range of topics as follows: frameworks for detecting malicious applications; algorithms for image quality assessment and image denoising based for image security and authorization; push notification-based malware; models for detecting potential insider threat; methods for financial fraud detection; security evaluation framework for military IOT devices; certificateless aggregate signature schemes; high-security interaction systems; secure incentive schemes for vehicular delay tolerant networks; ciphertext retrieval schemes; systems with secret key leakage-resilience; solutions for jammer localization in multihop wireless networks; homomorphic network coding signature schemes for multiple sources; cryptanalysis of compact-LWE and related lightweight public key encryption; smart trust management methods to detect on-off attacks; and network performance and security testing.

Conflicts of Interest

The editors declare that they have no conflicts of interest regarding the publication of this special issue.

Acknowledgments

As always, we appreciate the high quality submissions from authors and the support of the community of reviewers.

Karl Andersson
Ilsun You
Francesco Palmieri