Security and Communication Networks

Special Issue on
Social Security and Privacy for Social IoT

WILEY | Hindawi

CALL FOR PAPERS

The advent of the Internet of Things (IoT) opens up new vulnerabilities for both security and privacy due to the massive number of resource-constrained devices connected to the Internet (an estimate of over 50 billion devices by 2020).

The IoT paradigm is worsening overall security issues, due to the heterogeneity of connected IoT hardware platforms (i.e., different firmware types, revisions, etc.) as well as the variety of network technologies for interconnections (e.g., Bluetooth, Wi-Fi, IEEE 802.15.4, and Narrowband IoT (NB-IoT)), all with potential flaws and vulnerability to attacks.

IoT devices have to face many threats originating from the Internet and can also become a source of attacks towards the Internet as all "objects" can communicate with each other and, as a consequence, an attacker can have a high number of access points to discover vulnerabilities of systems in virtually all sectors of society, such as home automation, smart city, healthcare, and connected vehicles.

Recent Social Internet of Things (SIoT) models are considered where "objects" with frequent social relationships, similar characteristics, or similar interests can form social communities. As a consequence, new security and privacy issues and challenges have to be discussed within the SIoT context.

Sociality can have a significant impact on security, involving several different aspects which can be viewed in various ways. For example, sociality can be seen as a vulnerability due to fake accounts on social networks (such as Facebook, Twitter, YouTube, and Instagram), which can disseminate spam, malware, and fishing websites. On the other hand, it can be viewed as a form of defense against attacks because different social communities can be formed by tracking friends, kin, and colleagues that share content frequently via online social networks, and this social awareness of devices can be considered as a means to enhance the identification of trustworthy nodes.

This special issue invites researchers, developers, and industry experts to contribute original research and review articles on recent advances and future directions for security and privacy in social IoT scenarios.

Potential topics include but are not limited to the following:

- Social community-based security and privacy in heterogeneous IoT
- Social threat models and attack strategies for IoT
- Social reliability and reputation notions to model the level of trust among devices
- Social security and privacy support for 6LoWPAN
- Social distributed and resource-saving intrusion detection systems for IoT

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/sspi/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Laura Pierucci, University of Florence, Florence, Italy
laura.pierucci@unifi.it

Guest Editors
Houbing Song, Embry-Riddle Aeronautical University, Daytona Beach, USA
houbing.song@erau.edu

Hua Wang, Victoria University (VU), Melbourne, Australia
publicwang09@gmail.com

Submission Deadline
Friday, 31 May 2019

Publication Date
October 2019