Security and Communication Networks

Special Issue on

Computational Enablers for Security and Privacy for IoT

WILEY | Hindawi

CALL FOR PAPERS

While the evolution of Internet to IoT holds great promises for new set of applications for the citizens, increased efficiency, and a wider set of available services, security aspects must also be taken into consideration. IoT devices and technologies will be used in various domains (e.g., healthcare), where the interaction with the human being can generate safety hazards if the IoT devices are tampered or attacked from a security point of view. IoT devices must be protected from security attacks, but this can be a challenging task, considering the limited capabilities of IoT devices in terms of processing power, storage, and energy. As a consequence, the implementation and deployment of conventional cryptographic solutions can be challenging. At the same time, the data collected by the sensors must be accurate to support the IoT applications, especially the ones based on autonomic algorithms because they may not be able to take the right decisions in time on the basis of inaccurate sensor data. There is the need to investigate efficient computational enablers to support security of IoT in various functions. The term computational enablers include algorithms, software modules, or analytic programs. For example, signal processing algorithms could be used not only to check the plausibility of IoT sensor data but also to detect potential security attacks either by correlating the data from one sensor with other sensors or by analyzing the presence of anomalies or outliers in the sensor output. Machine learning and data analytics algorithms could be used to identify specific contexts and improve the identification and authentication of IoT devices on the basis of their physical features. Innovative cryptographic algorithms could also be investigated to address the specific limitations of IoT devices. Finally, there is the need to design and implement new security solutions, which are able to support IoT distributed environments (e.g., blockchain and lightweight cryptographic protocols).

We seek high-quality papers examining innovative and multidisciplinary methods and techniques to identify and/or mitigate security threats in relation to IoT networks and devices using machine learning and signal processing techniques. Papers will be peer-reviewed by independent reviewers and selected based on their quality and relevance to the topics of this special issue.

Potential topics include but are not limited to the following:

- Signal processing techniques to identify security threats to IoT devices and applications
- Physical layer authentication of IoT devices
- Application of machine learning algorithms to IoT security
- Automatic evaluation of security and privacy threats and benchmarking
- Analysis of data from IoT sensors to mitigate security threats
- Multiparty computation
- Secure consensus protocols and applications of the blockchain to secure computation
- Homomorphic cryptography and applications
- New applications for secure IoT
- Design of lightweight cryptographic protocols for IoT
- Detection of anomalies in IoT applications and their behavior

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

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

Lead Guest Editor
Gianmarco Baldini, European Commission Joint Research Centre, Ispra, Italy
gianmarco.baldini@ec.europa.eu

Guest Editors
Antonio Skarmeta, University of Murcia, Murcia, Spain
skarmeta@um.es

Claudio Gentile, University of Insubria, Varese, Italy
claudio.gentile@uninsubria.it

Jeff Voas, NIST, Gaithersburg, USA
jeff.voas@nist.gov

Shinsaku Kiyomoto, KDDI Research, Inc., Saitama, Japan
kiyomoto@kddi-research.jp

Submission Deadline
Friday, 29 September 2017

Publication Date
February 2018