Call for Papers

International Journal of Information Security
Special Issue on "IoT Security and Privacy"

The Internet is gradually transforming from a communication platform for conventional IT appliances into the Internet of Things (IoT), increasingly interconnecting many assorted devices and sensors. These devices are generally referred as IoT devices, and many of them are inexpensive and can be constrained in terms of energy, bandwidth and memory. The establishment of IoT ecosystems in various domains is bringing multiple benefits to human users and companies alike. Example of such domains include Smart Homes, Smart Cities, the Industrial Internet and even Intelligent Transportation Systems. However, the IoT as a whole – including related paradigms such as Machine-to-Machine (M2M) and Cyber-Physical Systems (CPS) – is susceptible to a multitude of threats. In fact, many IoT devices currently are insecure and have many security vulnerabilities. For example, many vulnerable IoT devices which have been infected with malware have subsequently become comprised into large botnets, resulting in devastating DDOS attacks. Consequently, ensuring the security of such IoT ecosystems – before, during, and after an attack takes place – is a crucial issue for our society at this moment.

This special issue aims to collect contributions by leading-edge researchers from academia and industry, show the latest research results in the field of IoT security and privacy, and provide valuable information to researchers as well as practitioners, standards developers and policymakers. Its aim is to focus on the research challenges and issues in IoT security. Manuscripts regarding novel algorithms, architectures, implementations, and experiences are welcome. Topics include but are not limited to:

- Secure protocols for IoT devices
- Privacy solutions and privacy helpers for IoT environments
- Trust frameworks and secure/private collaboration mechanisms for IoT environments
- Secure management and self-healing for IoT environments
- Operative systems security for IoT devices
- Security diagnosis tools for IoT devices
- Threat and vulnerability detection in IoT environments
- Anomaly detection and prevention mechanisms in IoT networks
- Case studies of malware analysis in IoT environments
- IoT forensics and digital evidence
- Testbeds and experimental facilities for IoT security analysis and research
- Standardization activities for IoT security
- Security and privacy solutions tailored to specific IoT domains and ecosystems

Important Dates
Manuscript Due: October 19, 2018
First Round of Reviews: December 21, 2018

Guest Editors
Takeshi Takahashi, National Institute of Information and Communications Technology, Tokyo, Japan; takeshi_takahashi@nict.go.jp
Bilhanan Silverajan, Tampere University of Technology, Tampere, Finland; bilhanan.silverajan@tut.fi
Ryan Ko, University of Waikato, Hamilton, New Zealand;ryan.ko@waikato.ac.nz
Said Tabet, EMC Corporation, MA, USA; said.tabet@dell.com
Rodrigo Roman Castro, Universidad de Málaga, Málaga, Spain; roman@lcc.uma.es

Springer