CALL FOR PAPERS

Springer Journal of Hardware and Systems Security
Special Issue on Secure and Trustworthy Computing Devices in the IoT Regime

GUEST EDITORS:
Yier Jin, yier.jin@eecs.ucf.edu, University of Central Florida
Sandip Ray, sandip.ray@nxp.com, NXP Semiconductors

AIMS and SCOPE:
The era of Internet-of-Things (IoT) is characterized by an environment in which we live in an ecosystem consisting of billions of smart, connected computing devices. Most of these devices are equipped with complex sensors that continuously collecting, analyzing, and communicating data pertaining to some of our most private and intimate activities, including sleep, health, location, social contacts, and browsing patterns. Security and privacy are clearly crucial to computing devices in this era. Security issues can come at different levels, including deployment issues that leave devices unprotected from cyber-attack, functional vulnerabilities in system design or implementation, an altered functionality by some player in the complex supply-chain, or side-channel issues exploitable by physical access to the device.
Furthermore, data collected by these devices have a complex communication path through switches, gateways, routers, and the cloud of servers and datacenters. Vulnerabilities in any point of this communication can compromise the entire IoT infrastructure, and have catastrophic consequences.

This Hass focuses on research challenges in ensuring security and trustworthiness in computing devices in the IoT regime, where the notion of “computing devices” is interpreted broadly to include not only sensor-attached “edge” devices but also to routers, gateways, and datacenters in contexts where they pertain to an IoT infrastructure. The aim is to provide a spectrum of challenges, approaches, and solutions, and provide an authoritative reference of the state of the art in security and trustworthiness issues for IoT.

TOPICS OF INTEREST:
The topics of interest for this special issue include, but are not limited to, the following:

- Hardware level exploitation of IoT
- Hardware-supported solutions for computing system protection
- SoC design for highly-secure IoT
- SoC security validation for IoT protection
- Cross-layer hardware/software attacks and protections on computing systems
- Hardware-supported trustworthy IoT design
- Data flow modeling for cyber physical system (CPS) security
- Security and privacy in smart routers and gateways
- Security-enhanced hardware structure for system protection
- Hardware security primitives including PUFs and Public PUFs
- Software level attacks on IoT leveraging hardware vulnerabilities
- Trusted computing platforms for smart devices in CPS
- Datacenter security challenges for IoT infrastructure
- Countermeasures for backdoors and in the software-hardware interface
• Formal verification for trusted hardware platform
• Trade-offs in IoT between security, privacy, performance, and energy constraints

Given that the goal of the issue is to provide an authoritative starting point for future research, we encourage authors to provide a comprehensive description of related research and state of practice.

IMPORTANT DATES:
Open for submissions in Springer Manuscripts: March 30, 2017
Closed for submissions: May 31, 2017
Results of first round reviews: August 15, 2017
Submission of revised manuscripts: September 15, 2017
Results of second round reviews: October 15, 2017
Publication material due: November 1, 2017

SUBMISSION GUIDELINES:
Prospective authors are invited to submit their manuscripts electronically after the “open for submissions” date, adhering to the Journal of Hardware and Systems Security guidelines (http://www.springer.com/engineering/circuits+%26+systems/journal/41635). Please submit your papers through the online system (https://www.editorialmanager.com/hass/default.aspx) and be sure to select the special issue or special section name. Manuscripts should not be published or currently submitted for publication elsewhere. Please submit only full papers intended for review, not abstracts, to the EditorialManager portal. If requested, abstracts should be sent by e-mail to the Guest Editors directly.