IEEE INTERNET OF THINGS JOURNAL

A joint publication of
IEEE Sensors Council, IEEE Communications Society, IEEE Computer Society, and IEEE Signal Processing Society

# CALL FOR PAPERS
# IEEE Internet of Things Journal Special Issue on Security and Privacy in Cyber-Physical Systems

A typical Cyber-Physical System (CPS) refers to the system that features a tight integration of computation, networking, and physical elements, and the Internet of Things (IoT) is the networking infrastructure of the CPS. CPS covers numerous smart world research areas that our daily life depends on, including smart transportation, smart electrical power grid, smart cities, smart medical systems, smart manufacturing systems, etc. While major research efforts have been conducted in improving the efficiency and reliability of CPS by using advanced information communication technologies, the risks of cyberspace security and privacy breaches in the CPS need to be seriously investigated before a massive deployment of CPS technologies can or should be realized.

Security and privacy issues continue to pose significant challenges. The CPS is a highly distributed and complicated system, and the operation and control of CPS depends on a complex cyberspace of computers, software, and communication technologies. The papers in this special issue will focus on the state-of-the-art research and the challenges in different aspects of security and privacy issues across various CPS domains, including energy, transportation, city infrastructure, public safety, unmanned autonomous vehicles, among others. We welcome papers as survey and application oriented papers. In this special issue, we solicit papers that cover numerous topics of interest that include, but are not limited to, the following:

- Security Vulnerability and Risk Assessment in CPS
- Theoretical Foundation and Models for CPS under Attacks
- Resiliency of CPS under Attacks
- Threat Monitoring and Detection in CPS
- Attack Attribution in CPS
- Integrated and Test Bed Validation for CPS
- Cloud Computing/Big Data Analytics for CPS Security
- Security and Performance Tradeoffs in CPS Design
- Privacy Issues in CPS
- Security, Privacy and Trust for CPS
- Secure IoT and CPS Architectures
- Security in Machine-to-Machine (M2M) for CPS
- Joint Security and Privacy aware Protocol Design in CPS
- Secure Network Control for CPS
- Data Mining, Machine Learning, Complex System Design for CPS

**Important Dates**

Submissions Deadline: **January 15, 2017** Notification of Acceptance: May 15, 2017
Final Manuscript Due: June 15, 2017 Publication Date: October 2017

**Submission**

All original manuscripts or revisions to the IEEE IoT Journal must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Solicited original submissions must not be currently under consideration for publication in other venues. Author guidelines and submission information can be found at http://iot.ieee.org/journal.

**Guest Editors**

Wei Yu (Co-Lead Guest Editor)
Towson University, USA
wyu@towson.edu

Xinwen Fu (Co-Lead Guest Editor)
Univ. of Massachusetts Lowell, USA
xinwenfu@cs.uml.edu

Houbing Song
West Virginia Univ., USA
h.song@ieee.org

Anastasios A. Economides
Univ. of Macedonia, Greece
economid@uom.gr

Minho Jo
Korea University, South Korea
minhojo@korea.ac.kr

Wei Zhao
University of Macau, China
weizhao@umac.mo