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 for IoT: the State of the Art

The Internet is becoming more and more ubiquitous. One central element of this trend is the existence of a massive network of interconnected wired/wireless physical objects/things/sensors/devices, which can interact in a rich set of manners through a worldwide communication and information infrastructure and provide value added services. The vision of such an Internet of Things (IoT) system, supported by industrial companies and governments globally, has the potential to mark an evolution that will surely have a great impact on our environments and our lives. Yet, the realization of a ubiquitous IoT also poses a number of challenges where security is among the top concerns. The globally interconnected physical objects inevitably result in a potentially enormous attack surface that can be easily exploited if without adequate protection. To enable strong security foundations for the ubiquitous IoT, plenty of factors need to be taken into account. Examples are data security, privacy, access control, information assurance, trust management, secure services interoperability, seamless integration, system heterogeneity, scalability, and mobility. This special issue solicits high-quality original research results about IoT that pertain to state-of-the-art security and privacy issues in various pervasive and ubiquitous scenarios. We encourage submissions on theoretical, practical, as well as experimental studies, from both academia and industry, related to all aspects of security for IoT. Topics of interests include (but are not limited to) the following categories:

- Secure IoT architecture
- IoT access control and key management
- Identification and privacy for IoT
- Smart phone enabled secure smart systems
- New cryptographic primitives for IoT
- Manage trust for IoT service interoperability
- Security on heterogeneous ecosystems
- Context-aware security design
- Data security and privacy in the IoT
- Intrusion detection and defense for IoT
- Joint security&privacy aware protocol design
- Failure detection, prediction, and recovery
- Secure data management within IoT
- Trusted computing technology and IoT
- Availability, recovery and auditing
- IoT related web services security
- Secure cyber-physical system
- Biometrics for the IoT

Important Dates

Submissions Deadline: February 15th, 2014
Revision Due: June 15th, 2014
Final Manuscript Due: August 15th, 2014
First Reviews Due: May 15th, 2014
Second Reviews Due/Acceptance letters: July 15th, 2014
Publication Date: October 15th, 2014

Submission

The special issue seeks submission of papers that present novel original results and findings on Security for 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. All manuscripts should be submitted through Manuscript Central: http://mc.manuscriptcentral.com/iot

Guest Editors

- Kui Ren, University at Buffalo, SUNY
  email: kuiren@buffalo.edu
- Pierangela Samarati, University of Milan
  email: pierangela.samarati@unimi.it
- Peng Ning, NCSU, Raleigh & Samsung Mobile
  email: pning@ncsu.edu
- Marco Gruteser, Rutgers University
  email: gruteser@winlab.rutgers.edu
- Yunhao Liu, Tsinghua University
  email: yunhaoliu@gmail.com

SI Publicity Chair: Cong Wang, City University of Hong Kong, email: congwang@cityu.edu.hk