Elsevier Journal of Computer Networks - *The International Journal of Computer and Telecommunications Networking*

Special Issue:

Security and Privacy for the Internet of Things[1]

Scope

The Internet of Things (IoT) is rapidly evolving from theory to real-life and large scale deployments. Examples include smart homes, industrial manufacturing, distributed sensing and tracking for logistics, and monitoring for transportation systems. While some IoT devices today provide basic security protection, security and privacy is very often centralized in the cloud and proprietary. Furthermore, large numbers of insecure devices can be integrated in a botnet and used to run denial of service attacks.

To foster trust, the myriad of IoT devices have to be designed and built with security and privacy in mind. As devices become smaller and may only use a limited amount of energy, guaranteeing security becomes a difficult task. Furthermore, the role the edge plays in protecting and scaling IoT devices is largely unclear.

This special issue is devoted to all aspects of IoT security and privacy, addressing the threats posed by the widespread use of the IoT.

Topics of interest include, but are not limited to:

- Security and privacy solutions for the IoT
- Secure and privacy-enhancing protocols for the IoT
- Distributed security for the cloud, the edge, and IoT devices
- Mitigation of security risks posed by large numbers of insecure devices.
- "Successful" attack instances in today's IoT and proposed mitigations
- Threat models and attack strategies in the IoT
- Malware and intrusion detection for the IoT
- Trust and collaboration among IoT devices
- Security management that supports scalable IoT security
- Self-healing and attack resilience for the IoT
- Industrial case studies and best practices including large-scale IoT test beds

---

[1] https://www.journals.elsevier.com/computer-networks/call-for-papers/special-issue-security-privacy-internet-of-things

- Embedded security and hardware security mechanism for protecting the IoT

Submission, Review, and Selection

Submitted articles must be original, unpublished, and not currently under review by other journals. Submitted articles must be written clearly, in good English, and should not exceed 20 pages (double-spaced). If a preliminary version of the paper was published in conference proceedings, the authors must clearly state this during the submission and the submitted manuscript must be a substantial extension of the earlier manuscript. In this case, the authors are also required to clearly explain the enhancements made in the journal version.

All manuscripts and any supplementary material should be submitted through Elsevier Editorial System (EVISE). The authors must select "IoT Security" when they reach the "Article Type" step in the submission process. The EVISE website is located at: https://www.evise.com/profile/#/AUTCON/login

Each submission will undergo a quick evaluation of its fit to the call, then a conference-style review by the members of the program committee, and a first feedback to authors with rejection, acceptance, or revision decision. If required, we plan shepherding papers that are conditionally accepted. The reviewers will check revised versions and a final decision will be made.

Important dates:

- Deadline for submission: August 06, 2018
- Feedback to authors: September 15, 2018
- Final version: October 15, 2018
- Final decision: November 01, 2018

Editorial Board:

- David Barrera (Polytechnique Montreal)
- Frank Piessens (KU Leuven)
- Hsu-Chun Hsiao (National Taiwan University)
- Kapil Singh (IBM Research)
- Mauro Conti (University of Padua)
- Nils Ole Tippenhauer (Singapore University)
- Nuno Neves (Universidade de Lisboa)
- Rodrigo Roman (University of Malaga)
- Samuel Marchal (Aalto University)
- Yier Jin (University of Florida)

Guest Editors:

- Andreas Wespi, IBM Research - Zurich, Switzerland
- Matthias Schunter, Intel Labs, Germany