Association for Computing Machinery

ACM Transactions on Internet Technology – Special Issue on **Human-Centered Security, Privacy, and Trust in the Internet of Things**

Special Issue Guest Editors

Dr. Mahmoud Barhamgi
(Corresponding GE)
Claude Bernard Lyon 1 University, France.
mahmoud.barhamgi@univ-lyon1.fr

Prof. Michael N. Huhns
University of South Carolina, USA.
huhns@sc.edu

Prof. Pınar Yolum
Utrecht University, The Netherlands. p.yolum@uu.nl

Dr. Charith Perera
Cardiff University, United Kingdom. pererac@cardiff.ac.uk

Important Dates

Manuscript submission: 30 June, 2020
First notification: 30 October, 2020
Revised version due: 15 December, 2020
Final notification: 30 January, 2021
Final submission: 30 February, 2021
Publication date: To be scheduled in 2021

Submission Instructions

Please refer to http://toit.acm.org/authors.cfm
Please select "*Human-Centered Security, Privacy, and Trust in the Internet of Things*" in the TOIT Manuscript Central website.

ACM TOIT Editor-in-Chief

Prof. Ling Liu
School of Computer Science, Georgia Institute of Technology
ling.liu@cc.gatech.edu

The Internet of Things (IoT) engenders exciting applications that touch almost all aspects of our lives. Examples include smart healthcare environments, intelligent homes, smart transportation networks, and adaptive city infrastructures. However, while such applications and systems promise to ease our lives, they also raise major security and privacy concerns for their users. The risks of privacy violation, data misuse, real-time surveillance, intrusions by malicious attackers as well as a lack of transparency prevent the wide adoption of those new technologies and systems.

To increase the trust of users in IoT applications and systems, and thereby pave the way for wider adoption, security and privacy protection solutions should provide more support for, and involvement of, users in the protection of their data and privacy, i.e., users should be supported to understand how their data is collected, processed, analyzed, stored, accessed and kept safe. They should also be able to exert their fundamental rights (as specified in applicable data protection laws, e.g., GDPR, CCPA) by controlling what data is collected about them and when, where, and for what purposes the collected data can be exploited, as well as the right to be forgotten. The users should also be provided with a transparent view into systems to verify, at any point of time, how their data is processed and being exploited.

The goal of this special issue is to collect recent advances, innovations, and practices in software and data engineering for building security and privacy protection systems, techniques, and solutions that provide effective involvement of users and increase their trust in IoT technologies. The topics of interest include, but are not limited to:

- Adaptive security and privacy to adapt to varying users and contexts;
- Solutions to privacy and security threats introduced by human behavior;
- Solutions to privacy and security threats introduced by the interaction between humans and IoT;
- Bringing transparency into IoT systems and software;
- Models and techniques for involving users in controlling their data;
- User privacy and security requirements;
- Privacy by design for IoT applications;
- Privacy risk assessment and visualization;
- Pragmatic data sharing decisions;
- Natural language for expressing data access/usage policy;
- Innovative models to acquire user consent;
- Tunable and adaptive data obfuscation;
- Assistive technology to promote more secure behavior and awareness of users;
- Models and techniques for engendering trust;
- Validating and explaining trust decisions in IoT systems.