Call for Papers

informatics

Special Issue Human Factors in Security and Privacy in IoT (HFSP-IoT)

We welcome submissions on the topic of the SECURITY and PRIVACY in the context of IoT, focusing on the human aspect

We would like to include papers about SOLUTIONS addressing ***vulnerabilities*** and potential ***privacy invasiveness*** of IoT devices

Editors:

Karen Renaud
(k.renaud@abertay.ac.uk)

Melanie Volkamer
(melanie.volkamer@kit.edu)

KEYWORDS:

- Human-Focused IoT Security/Privacy
- Human-Focused IoT Solutions to Security and Privacy Problems
- Acceptance of security and privacy IoT Solutions
- Awareness Raising
- Mental Models about IoT threats and risks
- Real life observations of human interactions with IoT devices
- Studies of IoT uses in developing countries that report specific security or privacy challenges

IoT includes smart home including devices such as digital assistants (e.g. google home and alexa) and smart health including devices such as fitness trackers. There are several aspects of high interest for this special issue

Aspects Include:

Investigations into the deployment of these solutions, especially studies related to acceptability of these solutions

Research into how humans are expected to interact with IoT devices to secure them, how they can be compromised

Research into how humans are expected to configure IoT devices to preserve their privacy, and perceptions of privacy-related IoT behaviours

Studies that reveal new security vulnerabilities or privacy violations facilitated by the design of the "Human-IoT" interface

Studies on users' awareness and perception of potential security and privacy threats and risks

DEADLINE

30 November 2018

This special issue of the Informatics journal welcomes submissions on the topic of the security and privacy in the context of IoT while focusing on the human aspect. IoT contains smart home including devices such as digital assistances (e.g. google home and alexa) and smart health, including devices such as fitness tracker. There are several aspects, which are of high interest for this special issue including:

- Investigations into the deployment of these solutions, especially studies related to acceptability of these solutions.;
- Research into how humans are expected to interact with IoT devices to secure them, how they can be compromised,
- Research into how humans are expected to configure IoT devices to preserve their privacy, and perceptions of privacy-related IoT behaviours.
- Studies that reveal new security vulnerabilities or privacy violations facilitated by the design of the "Human-IoT" interface.
- Studies on users' awareness and perception of potential security and privacy threats and risks

We would really like to include some solutions in our special issue: those that address vulnerabilities and potential privacy invasiveness of IoT devices. Our overall theme is IoT, and we will accept a wide range of papers related to either security or privacy of IoT devices, either in or out of the home.

We encourage authors to submit their original research articles, surveys, reviews, and viewpoint articles being labelled as position papers. This special issue welcomes applications, theories, models, and frameworks — whether conceptual, analytical, prescriptive, predictive, design-related, or otherwise—that are concerned with (but not limited to) the following topics as they relate to HFSP-IoT.

http://www.mdpi.com/journal/informatics/special_issues/HFSP-IoT