Security and Communication Networks

Special Issue on
Cybersecurity in the Internet of Things

WILEY | Hindawi

CALL FOR PAPERS

With the settlement of smartphones and tablets in modern societies, as well as the proliferation of an astronomic amount of other electronic devices such as wearables, e-Health sensors, electrical appliances, or vehicles (amidst others), all provided with Internet connection, all potentially dealing with sensitive information, and most of them mobile in essence, we are witnessing today the real advent of the Internet of Things (IoT). This new paradigm brings along many indubitable advantages, but also a nonnegligible number of security threats that should not go underestimated. Besides increasing in number, those threats are becoming more sophisticated and harmful (as it is the case of advanced persistent threats, or APTs), making it unfeasible for a human administrator to manually protect each and every device within the constellation of gadgets, artefacts, and computer systems of the IoT. Moreover, an alarming amount of the new solutions envisaged for the IoT pay higher attention to usability aspects, recklessly ignoring substantial security protection mechanisms, making the IoT an ideal playground for malicious hacking activities. Hence, it is imperative to find solutions aiming at the integral protection of the plethora of vulnerable devices within the IoT. Working on those solutions will help the wider adoption of these new technologies and help users to entrust them.

Thus, this Special Issue seeks high-quality original papers presenting innovative solutions dealing with cybersecurity in the field of IoT. In particular, novel techniques and mechanisms aimed at the security and privacy protection of these environments are welcome. Likewise, we encourage review articles describing and analyzing the current state of the art in this field. Papers with a strong cryptographic background will not be considered as part of this special issue.

Papers will be evaluated based on their originality, presentation, relevance, and contribution to the field of cybersecurity in the IoT, as well as their suitability to the special issue, and for their overall quality. The submitted papers have to describe original research which has not been published nor currently under review by other journals or conferences. Guest editors will make an initial determination of the suitability and scope of all submissions. Papers that either lack originality and clarity in presentation or fall outside the scope of the special issue will not be sent for review and authors will be promptly informed in such cases.

Potential topics include but are not limited to the following:

- Intrusion detection and prevention systems
- Malware analysis
- Privacy-preserving solutions
- Countermeasures solutions
- Seamless security solutions
- Threats and vulnerabilities
- Botnets analysis
- BYOD security
- Identity management
- Authorization and access control
- Trust and reputation management
- Machine learning-based solutions
- Security Information event management

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/cit/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Félix G. Mármol, University of Murcia, Murcia, Spain
felixgm@um.es

Guest Editors
Patricia A. Cabarcos, Universität Mannheim, Mannheim, Germany
pariasca@mail.uni-mannheim.de

Vijay Varadharajan, University of Newcastle, Newcastle, Australia
vijay.varadharajan@newcastle.edu.au

Submission Deadline
Friday, 5 January 2018

Publication Date
May 2018