INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

Call for Papers

Int. J. of Embedded Systems

CSS 2018: Special Issue on: "Lightweight Solutions for Cyberspace Security: Research Advances and Challenges"

Guest Editors:
Dr. Arcangelo Castiglione, University of Salerno, Italy
Prof. Xinyi Huang, Fujian Normal University, China
Prof. Laurence T. Yang, St. Francis Xavier University, Canada
Dr. Alessio Merlo, University of Genoa, Italy

While conventional security and privacy techniques work well on systems which have acceptable computational and memory capabilities, this does not apply to the modern, pervasively interconnected world. Today there are myriad embedded systems and sensor networks with very limited computational and memory capabilities. Such systems and networks are closely linked to sensitive infrastructures and strategic services such as the distribution of water and electricity, so designing and implementing privacy and security technologies in such environments is fundamental.

The introduction of lightweight techniques is essential to overcoming many of the problems arising from conventional security and privacy issues, such as constraints related to physical size, processing requirements, memory limitation and energy drain.

The main aim of this special issue is to present innovative research contributions aimed at addressing security and privacy issues within modern constrained network environments, and to provide a bridge for discussions and opportunities between the academic and industrial world.

The issue will carry revised and substantially extended versions of selected papers presented at the 10th International Symposium on Cyberspace Safety and Security (CSS 2018), but we are also inviting other experts to submit articles for this call.

Subject Coverage

Suitable topics include, but are not limited, to the following:

- Techniques to replace conventional cryptography
- New trends in the design of lightweight algorithms
- Adversarial modelling
- Side-channel analysis of existing protocols and implementations
- Low-cost side-channel countermeasures
- Lightweight privacy-preserving protocols and systems
- Intrusion detection and prevention schemes
- Vulnerability assessment and testing
- Formal methods for analysis of lightweight cryptographic protocols
- Security and privacy issues
- Tracing back mobile attackers
- Cryptographic hardware development
- Security and privacy issues in automotive technologies
- Security and privacy issues in smart cities

Notes for Prospective Authors

Submitted papers should not have been previously published nor be currently under consideration for publication elsewhere. (N.B. Conference papers may only be submitted if the paper has been completely re-written and if appropriate written permissions have been obtained from any copyright holders of the original paper).

All papers are refereed through a peer review process.

All papers *must* be submitted online. To submit a paper, please read our Submitting articles page.

Important Dates

Manuscripts due by: *30 December, 2018*

Notification to authors: *1 March, 2019*

Final versions due by: *1 May, 2019*