Lightweight Cryptography Workshop 2015

Gaithersburg, MD

July 20-21, 2015

http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm

CALL FOR SUBMISSIONS

There are several emerging areas in which highly constrained interconnected devices work in concert to accomplish some task. Examples include: sensor networks, healthcare, distributed control systems, the Internet of Things, cyber physical systems, and the smart grid. However, these constrained devices may not be able to support the NIST-approved strong cryptographic algorithms capable of protecting data for many years to come. NIST seeks to discuss the security and resource requirements of applications in constrained environments and potential future standardization of lightweight primitives.

NIST is soliciting papers, presentations, case studies, panel proposals, and participation from any interested parties. NIST will post the accepted papers and presentations on the workshop website; however, no formal workshop proceedings will be published.

Topics include, but are not limited to:

- Requirements and characteristics of real-world applications of lightweight cryptography
- Lightweight cryptography for RFID, SCADA, cyber-physical systems, and the Internet of Things
- Case studies of deployed systems
- Evaluation of threats, attacks and risks in lightweight cryptography
- Restrictions and protections to reduce the risk of using lightweight primitives
- Design, analysis and implementation of lightweight symmetric cryptographic primitives
- Lightweight public key cryptography
- Benchmarking of lightweight cryptographic algorithms in software and hardware
- Side channel attacks and countermeasures for constrained devices

Important dates

Submission deadline: April 1, 2015
Notification deadline: May 15, 2015
Registration deadline: July 1, 2015
Workshop: July 20-21, 2015

Submissions must be provided electronically in PDF format. Paper submissions should not exceed 15 pages. Proposals for presentations or panels should be no longer than 5 pages; panel proposals should identify possible panelists and an indication of which panelists have confirmed their participation.

Please submit the following information to lightweight-crypto2015@nist.gov:

- Contact details of the authors
- The finished paper, presentation or panel proposal in PDF format as an attachment.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce