Lightweight Cryptography Workshop 2016

Gaithersburg, Maryland
October 17-18, 2016

CALL FOR PRESENTATIONS

In 2013, NIST initiated the lightweight cryptography project to study the performance of the current NIST-approved cryptographic standards on constrained devices and to understand the need for a dedicated lightweight cryptography standard, and if the need is identified, to design a transparent process for standardization. In 2015, NIST held the first Lightweight Cryptography Workshop in Gaithersburg, MD, to get public feedback on the requirements and characteristics of real-world applications of lightweight cryptography. Currently, NIST is developing a report on lightweight cryptography, which will provide an overview of the project, as well as the plans for moving forward. In particular, NIST has decided to create a portfolio of dedicated lightweight algorithms through an open process similar to the selection of modes of operation of block ciphers. Algorithm recommendations will be associated with 'profiles' that target a class of devices and applications. NIST seeks to discuss issues related to potential future standardization process of lightweight primitives, including the proposed standardization process and profile construction.

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:

- Issues on the proposed standardization process
- Potential profiles
- 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: September 9, 2016
Notification deadline: September 23, 2016
Workshop: October 17-18, 2016

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-crypto2016@nist.gov:

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