NIST Threshold Cryptography Workshop 2019

Gaithersburg, MD

March 11-12, 2019

https://csrc.nist.gov/events/2019/NTCW19

CALL FOR SUBMISSIONS

NIST is interested in promoting the security of implementations of cryptographic primitives. This security depends not only on the theoretical properties of the primitives but also on the ability to withstand attacks on their implementations. It is thus important to mitigate breakdowns that result from differences between ideal and real implementations of cryptographic algorithms.

Threshold schemes for cryptographic primitives have the potential to strengthen the secrecy of cryptographic keys, as well as to enhance integrity and availability of the implemented primitives, including providing resistance against side-channel and fault attacks.

NIST seeks to discuss aspects of threshold cryptography (used as an umbrella term) in a wide range of application environments and the potential future standardization of threshold schemes for cryptographic primitives. Therefore, NIST is soliciting papers, presentations, 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:

- Security criteria, resource requirements and characteristics of real-world applications of threshold cryptographic systems
- Threshold techniques, including techniques related to secure multi-party computation and intrusion-tolerant distributed systems, both in hardware and software
- Case studies of deployed threshold systems
- Evaluation of security, reliability, threats and attacks in threshold cryptography
- Design, analysis and implementation of threshold schemes for cryptographic primitives
- Challenges in testing and validation of threshold cryptographic systems
- Benchmarking of threshold schemes in hardware and software
- Countermeasures against side-channel and fault attacks using threshold approaches
- Threshold cryptography for blockchain, cloud computing, hardware security modules (HSMs), and the Internet of Things (IoT)

Important dates

Submission deadline: December 17, 2018
Notification deadline: January 15, 2019
Registration deadline: February 18, 2019
Workshop: March 11-12, 2019

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 to ntcw2019@nist.gov:

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

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