Public Comments Received on

Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process

(Public Comment Period: May 14, 2018 to June 28, 2018)

From Sumanta Sarkar on May 24, 2018:

I have been following NIST's reports on lightweight cryptography. As I see that the report mentions about side channel analysis, but does not speak about differential fault analysis. Could you please let me know whether NIST wants submissions to be protected from both differential fault analysis and side channel analysis.

From Kevin R. Driscoll on May 27, 2018:

In contradiction to several previous comments on NIST LWC drafts, the current "Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process" draft is asking for a "one size fits all" LWC algorithm. "One size fits all" means not fitting very well in most cases. This is very true here. Per the previous comments and several papers in the literature, LWC has two distinct sub-domains:
1. very low-end hardware (e.g., RFIDs)
2. real-time software (particularly for 32-bit and 64-bit embedded processors)

The requirements are very different between the two. In particular, forcing these two sub-domains into a "one size fits all" solution could preclude algorithms for the real-time software sub-domain that could 10x to 100x better than candidates satisfying both sub-domains simultaneously. A difference of 2x or 3x might be excusable, but not 10x to 100x. Similar arguments likely hold for the reverse as well (e.g., RFIDS don't have the latency and speed of real-time software).

From Hongjun Wu on June 5, 2018:

1. It seems that the authentication security is not explicitly specified. For some message authentication codes, the authentication security downgrades as the amount of data being processed increases.
For the primary cipher with 64-bit authentication tag (line 270--271), I'd like to know what is the acceptable authentication security when the amount of data being processed under one key reaches around 2^50 bytes?

2. Is it mandatory for the primary cipher to resist the related-key attack?
I may prefer to assume that the key derivation for a lightweight cipher is secure.

3. Line 505: "The security strength ... will be considered under several models."
Is it possible to list those attack models?

From the Electronic Privacy Information Center on June 28, 2018:

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

"Request for Comments: Submission Requirements and Evaluation for the Lightweight Cryptography Standardization Process"

June 28, 2018

By notice published on May 14, 2018, the National Institute of Standards and Technology ("NIST") requested comments on a proposed process to solicit, evaluate, and standardize lightweight cryptographic algorithms that are suitable for use in constrained environments. The Electronic Privacy Information Center ("EPIC") submits these comments in support of NIST's effort to coordinate the standardization of cryptographic algorithms, subject to public comment. While we take no position on this specific proposal, we wish to express support for the NIST standard-setting process.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC was born out of the "Clipper Chip" campaign, the first Internet petition, and helped establish the freedom to use encryption in the United States.[1] Since that time, EPIC has pursued many efforts to safeguard this right.[2] EPIC also pursued many Freedom of Information Act cases to better inform the public about encryption policy. And EPIC has long supported the work of NIST on encryption standards. For example in 2014, EPIC and several organizations in sending a letter urging NIST to adopt "secure and resilient encryption standards, free from back doors or other known vulnerabilities."[3] EPIC recently submitted comments to NIST advising the agency to revise its Risk Management Framework to make clear that federal agencies are legally required to conduct privacy impact assessments.[4]

NIST's expertise in cryptography, its authority to accept public comment, and its ability to bring together leading experts to evaluate proposals is critical to the adoption of trustworthy

[1] EPIC, *The Clipper Chip*, https://www.epic.org/crypto/clipper/. John Markoff, *Gore Shifts Stance on Chip Code*, The New York Times (July 21, 1994), https://www.epic.org/crypto/clipper/;
[2] *See, e.g.,* EPIC, *Encryption & Liberty* 2000 (2000); *EPIC, Encryption & Liberty 1999* (1999); EPIC, *1996 Cryptography and Privacy Sourcebook* (1996); EPIC, *FBI Documents on Encryption* (1996), https://epic.org/crypto/ban/fbi_dox/.
[3] *See, e.g.,* Letter from EPIC et al. to Willie E. May, Assoc. Dir., NIST (Nov. 20, 2014), https://epic.org/misc/Coalition-NIST-Nov2014.pdf.
[4] EPIC Comments to NIST, Updating Risk Management Framework to Incorporate Privacy Considerations (June 22, 2018), https://epic.org/apa/comments/EPIC-NIST-PIA-June2018.pdf.

computer standards in the United States and around the world.[5] NIST's core responsibility under the Federal Information Security Management Act of 2002 is to develop, "information security standards and guidelines, including minimum requirements for federal information systems."[6] By combining both technical expertise and "cooperative work among private industrial organizations," NIST is well situated to advocate for privacy protections in the digital age.[7] For example, NIST SP 800-163, *Vetting the Security of Mobile Application*, recognizes that the "use of apps can potentially lead to serious security risks" and "is intended for. . . developers that are interested in understanding the types of software vulnerabilities that may arise in their apps during the app's software development life cycle."[8]

EPIC continues to support the NIST process established for the public development of technical standards. Participation by leading experts, industry groups, and public interest organizations helps ensure the safety, privacy, and security of a vast range of devices, networks and technologies. NIST's standard-setting process helps ensure the protection of privacy as small computing devices increasingly become ubiquitous.

Respectfully Submitted,

/s/ *Marc Rotenberg*
EPIC President

/s/ *Christine Bannan*
EPIC Administrative Law and Policy Fellow

/s/ *Jasmine Bowers*
EPIC PhDX Fellow

/s/ *Allison Gilley*
EPIC Law Clerk

/s/ *Evan Kratzer*
EPIC Law Clerk

---

[5] *See* EPIC, Computer Security Act of 1987, https://eforpic.org/crypto/csa/; Prepared Testimony of Marc Rotenberg on the Computer Security Act of 1987 and the Memorandum of Understanding Between the NIST and the NSA before the Subcommittee on Legislation and National Security, Committee on Government Operation, U.S. House of Representatives, May 9, 1989, https://epic.org/crypto/csa/Rotenberg-Testimony-CSA-1989.pdf

[6] *See* NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, ii, Authority (Apr. 2013) (describing source and scope of agency authority), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[7] 15 U.S.C. § 271(a)(5); *See also About NIST*, NIST.gov, https://www.nist.gov/about-nist.

[8] NIST, SP 800-163, *Vetting the Security of Mobile Applciations VI*, (Jan. 2015), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf.