ERICSSON

Date: September 30, 2021

Comments on SP 800-107 Rev. 1: Recommendation for Applications Using Approved Hash Algorithms

Dear NIST,

Thanks for your continuous efforts to produce well-written open-access security documents. FIPS 198-1, SP 800-22 Rev. 1a, SP 800-38D, SP 800-38E, and SP 800-107 Rev. 1 are all important documents that should be updated.

Please find below our comments on SP 800-107 Rev. 1:

- "FIPS 180-4"

  I assume this will be updated to [180-4] and [FIPS PUB 202]. I think the updated document should describe SHAKE and KMAC [800-185] in the same way as it discusses SHA-2 and HMAC. The SHAKE functions are used quite a lot (X.509, EdDSA, COSE, etc.) while the fixed-length SHA-3 hash algorithms seem to see limited practical use. Long-term I think NIST should consider referring to SHAKE as variable-length hash functions. Right now, the terminology is a bit confusing. NIST states that the variable-length KMAC is a keyed hash function but insists that SHAKE is not a hash function.

- It would be good if table 1 also listed security against length extension attacks. The low resistance against length extensions in many of the SHA-2 variants is not very nice and might come as a surprise to people using SHA-2.

- "A commonly acceptable length for the MacTag is 64 bits; MacTags with lengths shorter than 64 bits are discouraged."

  This is still a good general recommendation that does **not** require an update.

  The DTLS 1.3 draft [1] has recently forbidden 64-bit tags based on the single key integrity advantage. This measure is of theoretic interest but is not a good measure for security protocols where each connection has many keys and communication between two parties can use many connections. The process used in DTLS 1.3 leads to misleading results like that frequent rekeying the ideal MAC increases security [2].

  While using only 128-bit tags might be fine for many non-constrained systems, using 64-bit

Ericssson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN
Tel: +46 10 719 00 00
Fax: +46 10 719 95 27
VAT: SE556056625801
Reg no: 556056-6258
Visiting address
Torshamnsgatan 21 (Kista)

ERICSSON

Date: September 30, 2021

tags make perfect sense in constrained IoT. To break 64-bit security against online brute force an attacker would on average have to send 4.3 billion messages per second for 68 years, which is totally infeasible in constrained IoT radio technologies.

[1] https://datatracker.ietf.org/doc/html/draft-ietf-tls-dtls13

[2] https://datatracker.ietf.org/meeting/110/materials/slides-110-saag-analysis-of-usage-limits-of-aead-algorithms-00

Best Regards,
John Preuß Mattsson,
Senior Specialist, Ericsson

Ericssson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN
Tel: +46 10 719 00 00
Fax: +46 10 719 95 27
VAT: SE556056625801
Reg no: 556056-6258
Visiting address
Torshamnsgatan 21 (Kista)