Public Comments on FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC)

Comment period: August 6, 2021 - October 1, 2021

On August 6, 2021, NIST's Crypto Publication Review Board initiated a review of FIPS 198-1, *The Keyed-Hash Message Authentication Code* (HMAC) (July 2008). This document includes the public comments received during the comment period from August 6, 2021 to October 1, 2021.

More details about this review are available from NIST's Crypto Publication Review Project site.

LIST OF COMMENTS

1. Comments from Daniel Niu, August 27, 2021 2
2. Comments from Canadian Centre for Cyber Security (CCCS), September 1, 2021 3
3. Comments from Mridul Nandi, Indian Statistical Institute, September 20, 2021 4
4. Comments from John Preuß Mattsson, Ericsson, September 30, 2021 5

1. Comments from Daniel Niu, August 27, 2021

HMAC was one that stands out in its kind in that it allowed keys of arbitrary length key to be used in computation of MAC Tag.

While being capable of specifying a key of arbitrary length is a nice feature in some way, it creates implementation burden when trying to unify the programming interface of a PRF. For example, with CMAC, the key is fixed length; for non-NIST-approved systems using keyed BLAKE2 (successor of one of the SHA-3 finalist), there is a length limit on the key.

Additionally, an erratum had been reported for RFC-2104 which FIPS-198 is based on, making a new requirement that keys whose length is bigger than the block size of the hash function be not used. The URL of the erratum is https://www.rfc-editor.org/errata/eid4809

I suggest NIST import the RFC erratum, specifying that too-large keys should not be used, and possibly consider a similar key-length limit for KMAC as well.

Regards,

DannyNiu/NJF.

2. Comments from Canadian Centre for Cyber Security (CCCS), September 1, 2021

As FIPS 140-2 will be retired as of September 21, 2021. Reference to it should be replaced by references to FIPS 140-3.

Comments on SP 800-107r1:

A number of other revisions should be included in the document:

- FIPS 186-3 was updated to FIPS 186-4 (with revision 5 in draft form, potentially coming out soon)
- SP 800-56A was updated to Revision 3
- SP 800-56B was updated to Revision 2
- SP 800-56C was updated to Revision 2
- SP 800-57 Part 1 was updated to Revision 5
- SP 800-90A was updated to Revision 1
- SP 800-131A was updated to Revision 2
- SP 800-133 was updated to Revision 2
- SP 800-135 was updated to Revision 1

In Section 4.1, page 7, discussion on security properties and usage of SHA-1, updated and complete reference [1] could be used to point out that the security proof for HMAC does not rely on collision resistance of the underlying PRF.

Footnote 4 on page 14 discusses exclusion of impractical collision attacks from this document. Researchers since found existing generic attacks similarly impractical [2, 3] and this information can be included in a similar footnote.

References:

[1] Bellare, M. New Proofs for NMAC and HMAC: Security without Collision Resistance. J Cryptol 28, 844–878 (2015). https://doi.org/10.1007/s00145-014-9185-x

[2] Peyrin T., Sasaki Y., Wang L. (2012) Generic Related-Key Attacks for HMAC. In: Wang X., Sako K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34961-4_35

[3] Guo J., Peyrin T., Sasaki Y., Wang L. (2014) Updates on Generic Attacks against HMAC and NMAC. In: Garay J.A., Gennaro R. (eds) Advances in Cryptology – CRYPTO 2014. CRYPTO 2014. Lecture Notes in Computer Science, vol 8616. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44371-2_8

3. Comments from Mridul Nandi, Indian Statistical Institute, September 20, 2021

Hi,

I have recently found that the constants ipad and opad in HMAC are redundant. The detailed analysis can be found in https://eprint.iacr.org/2021/097

Moreover, I have shown that the security of HMAC (and NMAC) remains good even if the underlying compression function becomes weak up to a certain level.

Thanks and regards,

Mridul Nandi

Professor, Applied Statistics Unit

Indian Statistical Institute, Kolkata

4. Comments from John Preuß Mattsson, Ericsson, September 30, 2021

Dear NIST,

Thanks for your continuous efforts to produce well-written open-access security documents. Please find attached our comments on FIPS 198-1.

Best Regards,

John Preuß Mattsson,

Senior Specialist, Ericsson

ERICSSON

Date: September 30, 2021

Comments on FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC)

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 FIPS 198-1:

- It would be good to also mention that HMAC can also be used as a pseudorandom function / key-derivation function. This is currently missing. It would also be good if the specification gives a reference to SP 800-56C Rev. 2 as this is likely useful for many readers.

- ”HMAC shall use an Approved cryptographic hash function [FIPS 180-3].”

  I assume this will be updated to [180-4] and [FIPS PUB 202]. It would be good if the specification also gives a reference to KMAC [800-185], which might be a more efficient solution then HMAC-SHA3 in many cases.

Best Regards,
John Preuß Mattsson,
Senior Specialist, Ericsson