

Internet Engineering Task Force
Internet-Draft
Updates: [5905](#) (if approved)
Intended status: Standards Track
Expires: July 8, 2019

A. Malhotra
S. Goldberg
Boston University
January 4, 2019

**Message Authentication Code for the Network Time Protocol
draft-ietf-ntp-mac-06**

Abstract

[RFC 5905](#) states that Network Time Protocol (NTP) packets should be authenticated by appending the NTP data to a 128-bit key, and hashing the result with MD5 to obtain a 128-bit tag. This document deprecates MD5-based authentication, which is considered to be too weak, and recommends the use of AES-CMAC as in [RFC 4493](#) as a replacement.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 8, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4.e](#) of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1.](#) Introduction [2](#)
- [1.1.](#) Requirements Language [2](#)
- [2.](#) Deprecating the use of MD5 [2](#)
- [3.](#) Replacement Recommendation [3](#)
- [4.](#) Motivation [3](#)
- [5.](#) Test Vectors [3](#)
- [6.](#) Security Considerations [3](#)
- [7.](#) Acknowledgements [4](#)
- [8.](#) IANA Considerations [4](#)
- [9.](#) References [4](#)
- [9.1.](#) Normative References [4](#)
- [9.2.](#) Informative References [4](#)
- Authors' Addresses [5](#)

1. Introduction

[RFC 5905](#) [[RFC5905](#)] states that Network Time Protocol (NTP) packets should be authenticated by appending the NTP data to a 128-bit key, and hashing the result with MD5 to obtain a 128-bit tag. This document deprecates MD5-based authentication, which is considered to be too weak, and recommends the use of AES-CMAC [[RFC4493](#)] as a replacement.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

2. Deprecating the use of MD5

[RFC 5905](#) [[RFC5905](#)] defines how the MD5 digest algorithm in [RFC 1321](#) [[RFC1321](#)] can be used as a message authentication code (MAC) for authenticating NTP packets. However, as discussed in [[BCK](#)] and [RFC 6151](#) [[RFC6151](#)], this is not a secure MAC and therefore MUST be deprecated.

3. Replacement Recommendation

If NTP authentication is implemented, then AES-CMAC as specified in [RFC 4493](#) [[RFC4493](#)] MUST be computed over all fields in the NTP header, and any extension fields that are present in the NTP packet as described in [RFC 5905](#) [[RFC5905](#)]. The MAC key for NTP MUST be 128 bits long AES-128 key and the resulting MAC tag MUST be at least 128 bits long as stated in [section 2.4 of RFC 4493](#) [[RFC4493](#)]. NTP makes this transition possible as it supports algorithm agility as described in [Section 2.1 of RFC 7696](#) [[RFC7696](#)].

The hosts who wish to use NTP authentication share a symmetric key out-of-band. So they MUST implement AES-CMAC and share the corresponding symmetric key. A symmetric key is a triplet of ID, type (e.g. MD5, AES-CMAC) and the key itself. All three have to match in order to successfully authenticate packets between two hosts. Old implementations that don't support AES-CMAC will not accept and will not send packets authenticated with such a key.

4. Motivation

AES-CMAC is recommended for the following reasons:

1. It is an IETF standard that is available in many open source implementations.
2. It is immune to nonce-reuse vulnerabilities (e.g. [[Joux](#)]) because it does not use a nonce.
3. It has fine performance in terms of latency and throughput.
4. It benefits from native hardware support, for instance, Intel's New Instruction set GUE [[GUE](#)].

5. Test Vectors

For test vectors and their outputs refer to [Section 4 of RFC 4493](#) [[RFC4493](#)]

6. Security Considerations

Refer to the Appendices A, B and C of NIST document on recommendation for the CMAC mode of authentication [[NIST](#)] and Security Considerations Section of [RFC 4493](#) [[RFC4493](#)] for discussion on security guarantees of AES-CMAC.

7. Acknowledgements

The authors wish to acknowledge useful discussions with Leen Alshenibr, Daniel Franke, Ethan Heilman, Kenny Paterson, Leonid Reyzin, Harlan Stenn, and Mayank Varia.

8. IANA Considerations

This memo includes no request to IANA.

9. References

9.1. Normative References

- [NIST] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", <<https://www.nist.gov/publications/recommendation-block-cipher-modes-operation-cmac-mode-authentication-0>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC4493] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", [RFC 4493](#), DOI 10.17487/RFC4493, June 2006, <<https://www.rfc-editor.org/info/rfc4493>>.
- [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", [RFC 5905](#), DOI 10.17487/RFC5905, June 2010, <<https://www.rfc-editor.org/info/rfc5905>>.

9.2. Informative References

- [BCK] Bellare, M., Canetti, R., and H. Krawczyk, "Keyed Hash Functions and Message Authentication", in Proceedings of Crypto'96, 1996.
- [GUE] Geuron, S., "Intel Advanced Encryption Standard (AES) New Instructions Set", <<https://www.intel.com/content/dam/doc/white-paper/advanced-encryption-standard-new-instructions-set-paper.pdf>>.
- [Joux] Joux, A., "Authentication Failures in NIST version of GCM", <http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/800-38_Series-Drafts/GCM/Joux_comments.pdf>.

- [RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", [RFC 1321](#), DOI 10.17487/RFC1321, April 1992, <<https://www.rfc-editor.org/info/rfc1321>>.
- [RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", [RFC 6151](#), DOI 10.17487/RFC6151, March 2011, <<https://www.rfc-editor.org/info/rfc6151>>.
- [RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", [BCP 201](#), [RFC 7696](#), DOI 10.17487/RFC7696, November 2015, <<https://www.rfc-editor.org/info/rfc7696>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

Authors' Addresses

Aanchal Malhotra
Boston University
111 Cummington St
Boston, MA 02215
US

Email: aanchal4@bu.edu

Sharon Goldberg
Boston University
111 Cummington St
Boston, MA 02215
US

Email: goldbe@cs.bu.edu

