Internet Engineering Task Force (IETF)
Request for Comments: 8573
Updates: 5905
Category: Standards Track
ISSN: 2070-1721

A. Malhotra
S. Goldberg
Boston University

June 2019

Message Authentication Code for the Network Time Protocol

Abstract

The Network Time Protocol (NTP), as described in RFC 5905, states that NTP packets should be authenticated by appending 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 too weak, and recommends the use of AES-CMAC as described in RFC 4493 as a replacement.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8573.

Table of Contents

1. Introduction

The Network Time Protocol [RFC5905] states that NTP packets should be authenticated by appending 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 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 described 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 an AES-128 key that is 128 bits in length, and the resulting MAC tag

MUST be at least 128 bits in length, 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 that 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 and 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 specification that is supported 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. IANA Considerations

This document has no IANA actions.

7. Security Considerations

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

8. References

8.1. Normative References

[NIST] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", NIST Special Publication 800-38B, DOI 10.6028/NIST.SP.800-38B, October 2016, <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>.

[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>.

8.2. Informative References

[BCK] Bellare, M., Canetti, R., and H. Krawczyk, "Keying Hash Functions and Message Authentication", Advances in Cryptology - Crypto 96 Proceedings, Lecture Notes in Computer Science, Vol. 1109, N. Koblitz ed, Springer-Verlag, 1996.

[GUE] Geuron, S., "Intel Advanced Encryption Standard (AES) New Instructions Set", May 2010, <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>.

Acknowledgements

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

Authors' Addresses

Aanchal Malhotra
Boston University
111 Cummington St
Boston, MA 02215
United States of America

Email: aanchal4@bu.edu

Sharon Goldberg
Boston University
111 Cummington St
Boston, MA 02215
United States of America

Email: goldbe@cs.bu.edu