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.

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.
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
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


8.2. Informative References


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