NTP Working Group
Internet Draft
Intended status: Standards Track
Updates: 5905
Expires: September 2016

D. Mayer
Network Time Foundation
H. Stenn
Network Time Foundation

March 14, 2016

The Network Time Protocol Version 4 (NTPv4) MAC Extension Field
draft-mayer-ntp-mac-extension-field-00.txt

Abstract

The Network Time Protocol Version 4 (NTPv4) defines in RFC5905 the optional usage of Message Authentication Code (MAC). The MAC is an optional component of the NTP packet at the end of the packet. There can only be one MAC segment in the packet but there is no way of knowing if the last data segment at the end of an NTP packet is a MAC or an extension field, which is also defined in RFC5905. This draft defines a MAC extension field which will allow the existing MAC segment to be moved into an extension field and have a known length and deprecates the existing MAC.

Table of Contents

1. Introduction

The NTP packet format consists of a set of fixed fields that may be followed by some optional fields. Two types of optional fields are currently defined, a Message Authentication Code (MAC), and extension fields, as defined in Section 7.5 of [RFC5905].

If a MAC is used it resides at the end of the packet. This field has a length which depends on the digest algorithm being used. While extension fields have a known length specified in the extension field header, there is no simple way to unequivocally know if the final extra data segment in an NTP packet is a MAC or if it is an extension field. There is also no currently implemented way to pad the length of a MAC to make it difficult to determine the digest algorithm being used.

This document creates a MAC extension field to remove this ambiguity, clearly defining a MAC in an extension field with known size, and

allows us the possibility of deprecating the MAC as described in [RFC5905]. The content of the MAC extension field is almost identical to the existing MAC field but with a size specified in the extension field and the ability to have multiple MAC's within the extension field for different digest algorithms. We note that the only current potential use for multiple MAC algorithms would be for certain broadcast scenarios. By deprecating the original MAC field all parts of the NTP packet will have well-specified lengths.

2. Conventions Used in this Document

2.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

2.2. Terms & Abbreviations

NTPv4	Network Time Protocol Version 4 [RFC5905]
MAC	Message Authentication Code
Legacy MAC	MAC as defined in RFC5095

3. MAC Extension Field

The MAC extension field is designed to allow one or more MAC digests to be present within the MAC extension field. The MAC extension field contains the unsigned number of MACs present followed by the unsigned size of each MAC. The number of MACs listed in the MAC COUNT in this extension field MUST be greater than zero. The MAC extension field SHOULD be the last extension field in the packet and a legacy MAC at the end of the packet is OPTIONAL. The extension field MAC supplants the use of a legacy MAC. All new extension fields that require a MAC SHOULD use this MAC extension field, if the recipient implements the MAC extension field. The MACs present in the extension field should perform the digest on all parts of the packet up to but not including the MAC extension field. A legacy MAC MAY be present at the end of the extension fields provided it covers all extension fields including the MAC extension field and is present only for reasons of interoperability with servers that do not understand the new MAC extension field but require a MAC for authentication of the packet. The layout of the data in a MAC extension field is as follows:

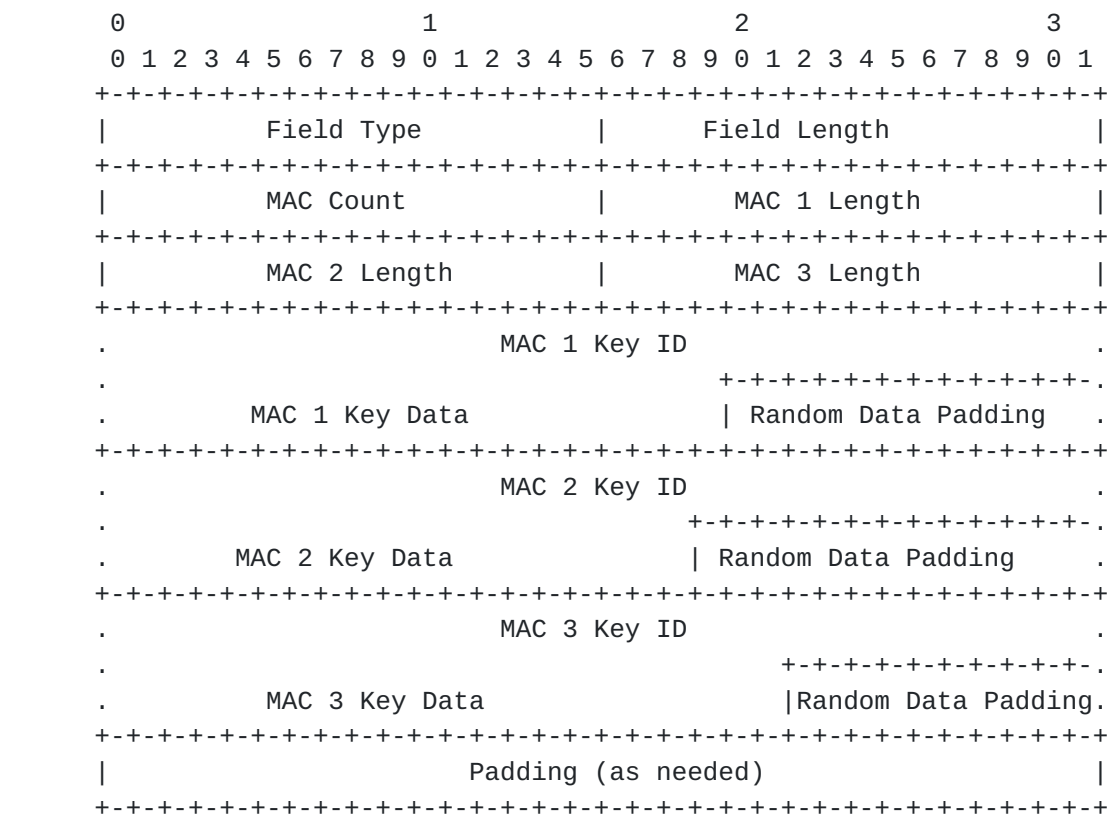

Figure 1: MAC Extension Field Format

A Field Type of 0 and a Length of 0 means this extension field is a CRYPTO-NAK, as defined by RFC5905. Otherwise, a Field Type value of TBD identifies this extension field as a MAC Extension field. The MAC Count is an unsigned 16-bit field, as is each MAC length field. If there are an even number of MACs specified there is an unused 16-bit field which SHOULD be 0x0000 at the end of the set of MAC length values so that the subsequent MAC data is longword (4-octet) aligned. Each MAC SHALL be padded so that any subsequent MAC starts on a 4-octet boundary.

A MAC SHOULD not be present if there is a crypto-NAK present in the packet.

Each MAC within the extension field consists of a 32-bit key identifier which SHOULD be unique to the set of key identifiers in this MAC extension field followed by ((MAC Length) - 4) octets of data, optionally followed by random octets to pad the key data to the length specified earlier in the extension field. That key identifier

is a shared secret which defines the algorithm to be used and a cookie or secret to be used in generating the digest. The MAC digest is produced by hashing the data from the beginning of the NTP packet up to but not including the start of the MAC extension field. The calculation of the digest SHOULD be a hash of this data concatenated with the 32-bit keyid (in network-order), and the key. When sending or receiving a key identifier each side needs to agree on the key identifier, algorithm and cookie to be used to produce the digest along with the digest lengths. Note that the sender may send more bytes than are required by the digest algorithm. This would be done to make it more difficult for a casual observer to identify the algorithm being used based on the length of the data. The digest data begins immediately after the key ID, and any padding octets SHOULD be random.

MAC values should be processed until either one of the MACs is validated, in which case the entire packet up to the beginning of the MAC extension field is considered to be validated, or no more MAC values are left to be validated, in which case the NTP packet is considered to have failed MAC validation.

4. Security Considerations

The security considerations of time protocols in general are discussed in [RFC7384], and the security considerations of NTP are discussed in [RFC5905].

Digests MD5, DES and SHA-1 are considered compromised and should not be used [COMP].

If possible each MAC length should be at least 68 octets long to allow for 4 octets of key ID and at least 64 octets of digest and random padding. This means that for SHA-256 digests there are 4 octets of key ID, 32 bytes digest and 32 random octets of padding. Using larger minimum MAC lengths makes it difficult for an attacker to know which digest algorithms are used.

5. IANA Considerations

IANA is requested to allocate the NTP extension Field Type value of 0x0000 for CRYPTO-NAK.

IANA is requested to allocate an NTP extension Field Type value for the MAC extension. We recommend 0x3003.

6. Acknowledgments

The authors gratefully acknowledge Dave Mills for his insightful comments.

This document was prepared using 2-Word-v2.0.template.dot.

7. References

7.1. Normative References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5905] Mills, D., Martin, J., Burbank, J., Kasch, W., "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

7.2. Informative References

[RFC5906] Haberman, B., Mills, D., "Network Time Protocol Version 4: Autokey Specification", RFC 5906, June 2010.

[COMP] TBF

Authors' Addresses

Danny Mayer
Network Time Foundation
PO Box 918
Talent OR 97540

Email: mayer@ntp.org

Harlan Stenn
Network Time Foundation
PO Box 918
Talent OR 97540

Email: stenn@nwtime.org