Network Time Protocol Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 24, 2016

D. Franke
Akamai

June 22, 2016

Clarifying Processing Expectations for Packets with keyid 0 in the Network Time Protocol Version 4 draft-dfranke-ntp-keyid0-00

Abstract

This memo clarifies that when a Network Time Protocol Version 4 packet has a keyid field of zero, the MAC is present solely to satisfy certain syntactic constraints, and is to be ignored.

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 http://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 December 24, 2016.

Copyright Notice

1. Introduction

A Network Time Protocol Version 4 (NTPv4) packet consists of 48 octets of required fields, followed by zero or more extension fields, possibly followed by a keyid field and a MAC. RFC 5905 [RFC5905] (section 7.5) specifies that the MAC "is always present when an extension field is present". RFC 7822 [RFC7822] relaxes this requirement by permitting the keyid and MAC fields to be omitted, provided that the last extension field has a length of at least 28 octets. This minimum length requirement is necessary to prevent syntactic ambiguity.

Neither RFC 5905 nor RFC 7822 provides any clear guidance on what to do when it is necessary to construct a packet which contains at least one extension field but none with a length of 28 octets or more, and no key has been agreed which could be used to compute a valid MAC. This memo resolves this situation by codifying the convention, already observed by the RFC 5905 reference implementation and other existing implementations, that a keyid field of zero is a dummy value indicating that the MAC field is to be ignored.

2. Requirements 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 RFC 2119 [RFC2119].

3. Processing Expectations

In an NTPv4 packet, a keyid field with a value of zero denotes that the keyid field and the MAC field which follows it have been inserted solely to satisfy a syntactic requirement for the presence of a MAC field. Implementations which receive such a packet MUST process it in the same manner that they would if the keyid and MAC fields were omitted (supposing this were syntactically possible). In particular, implementations MUST NOT attempt to verify the MAC, and MUST NOT respond to the sender with a crypto-NAK.

4. Security Considerations

The security considerations of time protocols in general are discussed in RFC 7384 [RFC7384], and the security considerations of NTP are discussed in RFC 5905 [RFC5905].

Legacy MAC fields containing dummy values do not contribute any information regarding the authenticity or inauthenticity of an NTP packet. NTP packets with dummy MAC fields MAY prove their authenticity by other mechanisms, e.g.

[draft-mayer-ntp-mac-extension-field]. See the previously-cited RFC 7384 and RFC 5905 for discussion of the security considerations surrounding accepting unauthenticated time packets.

Whenever two cooperating principals have conflicting processing expectations for a similar message, "confused deputy" vulnerabilities may arise [confused-deputy]. Without speculating as to any specifics as to how this class of vulnerability could arise from this instance of confusion, by making the processing expectations clear we preclude the possibility of it doing so.

5. IANA Considerations

None.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[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, <http://www.rfc-editor.org/info/rfc5905>.

[RFC7822] Mizrahi, T. and D. Mayer, "Network Time Protocol Version 4 (NTPv4) Extension Fields", RFC 7822, DOI 10.17487/RFC7822, March 2016, <http://www.rfc-editor.org/info/rfc7822>.

6.2. Informative References

[RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in

Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384, October 2014, <http://www.rfc-editor.org/info/rfc7384>.

[confused-deputy]
Hardy, N., "The Confused Deputy: (or why capabilities might have been invented)", ACM SIGOPS Operating Systems Review Volume 22 Issue 4, pp. 36-38, October 1988.

[draft-mayer-ntp-mac-extension-field]
Mayer, D. and H. Stenn, "The Network Time Protocol Version 4 (NTPv4) MAC Extension Field", March 2016, <https://datatracker.ietf.org/doc/draft-mayer-ntp-mac-extension-field/>.

Work in progress.

Author's Address

Daniel Fox Franke
Akamai Technologies, Inc.
150 Broadway
Cambridge, MA 02142
United States

Email: dafranke@akamai.com
URI: https://www.dfranke.us