Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: January 3, 2019

H. Stenn
D. Mills
P. Prindeville
Network Time Foundation
July 2, 2018

Network Time Protocol: Secure Network Time
draft-stenn-ntp-secure-network-time-00

Abstract

The proposal specifies a means for NTP instances that can establish a TCP connection between themselves to create secure ephemeral keys. With the known weaknesses of the public-key security protocol, Autokey, which is defined by RFC 5906 [RFC5906], a replacement for Autokey that supports at least Client/Server and Symmetric modes must be provided.

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 January 3, 2019.

Copyright Notice

Table of Contents

1. Introduction

From almost the beginning, NTP has provided a mechanism to authenticate an NTP packet. To date, that mechanism is a Message Authentication Code, or MAC. The MAC is comprised of two subfields, a 32-bit keyID and a signature. A keyID with a value between 1 and 65535, inclusive, is a symmetric key. A keyID with a value greater than 65535 is not provided by the symmetric key file, and has traditionally been negotiated ephemerally, with Autokey, defined by RFC 5906 [RFC5906], being one example.

The mechanism by which keys are exchanged between NTP instance can be thought of as a black-box exchange. One of these black-box key exchange mechanisms is "the way the ntp.keys file containing symmetric keys is distributed." Another way keys have been exchaned is via Autokey.

This Secure Network Time proposal uses the NTP TCP Services mechanism to perform key exchange, follwed by negotiation of a keyID, a hash algorithm, and a secret key over a TLS connection. Once this has been done, each participant can use the keyID, hash algorithm, and secret key to provide MAC protection for NTP packets, using ephemeral keys that can be re-negotiated as-needed.

Should additional security measures be desired, for example using a cookie as additional replay prevention, that can be easily provided.

1.1. Requirements Language

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].

2. Secure Network Time

Secure Network Time uses "NTP TCP Services" to perform key exchange over a TLS connection, followed by an agreement on a keyID, hash algorithm, and a secret. With the secure communication of a keyID, a cryptographically strong hash algorithm, and a secret of sufficient strength, we have an ephemeral key exchange mechanism that provides MAC authentication for NTP packets.

3. IANA Considerations

TBD

4. Security Considerations

Additional information TBD

5. 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, <https://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, <https://www.rfc-editor.org/info/rfc5905>.

[RFC5906] Haberman, B., Ed. and D. Mills, "Network Time Protocol Version 4: Autokey Specification", RFC 5906, DOI 10.17487/RFC5906, June 2010, <https://www.rfc-editor.org/info/rfc5906>.

Authors' Addresses

Harlan Stenn
Network Time Foundation
P.O. Box 918
Talent, OR 97540
US

Email: stenn@nwtime.org

David L. Mills
Network Time Foundation
P.O. Box 918
Talent, OR 97540
US

Email: mills@udel.edu

Philip Prindeville
Network Time Foundation
P.O. Box 918
Talent, OR 97540
US

Email: prindeville@ntp.org