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: TCP Services: Key Exchange
draft-stenn-ntp-tcp-services-keyexchange-00

Abstract

This document describes the Key Exchange commands that are included in the NTP TCP Services protocol, which is used to implement the Secure Network Time protocol.

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.

Table of Contents

1. Introduction

The NTP Secure Network Time proposal relies on the secure pre-exchange of information to create and validate NTP MACs,

This secure pre-exchange is performed using NTP TCP Services.

This document describes that protocol.

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. NTP TCP Services: Key Exchange

To perform the key exchange for Secure Network Time, one side opens a TCP connection to the other host, performs any initial handshake, and SHOULD issue a STARTTLS directive to create a secure channel between the two processes.

Once that has been done, ...

RFC 5705 [RFC5705]

RFC 7301 [RFC7301]

[Show how this works for Client/Server mode]

[Show how this works for symmetric mode]

[Show how this work for manycast/multicast]

[Show how this would work for broadcast mode where the client can open a connection to the server]

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>.

[RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, DOI 10.17487/RFC5705, March 2010, <https://www.rfc-editor.org/info/rfc5705>.

[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>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

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