NTS4PTP

Network Time Security for the Precision Time Protocol

Status Report

Martin Langer, Rainer Bermbach

IETF 116 - NTP working group, March 28, 2023
NTS4PTP
very short recap

• What is NTS4PTP about and what are the objectives?
  – We want a security solution for PTPv2.1
    ▪ Protecting PTP multicast and PTP mixed multicast/unicast \( \rightarrow 1:n \) connections
    ▪ Protecting PTP negotiated unicast \( \rightarrow 1:1 \) connections
  – Using NTS as a basis
    ▪ Advantage: Providing a common security protocol for NTP and PTP
NTS4PTP

current status

• No much progress in 2022
  – Current draft: draft-langer-ntp-nts-for-ptp-05
  – Only small changes

• Reasons
  – Doctoral thesis
  – Analyses and discussions about the protocol merge: NTS4UPTP and NTS4PTP
  – Job change (Ostfalia to PTB)
  – Supervise of a first PoC of NTS4PTP

• Work on NTS4PTP resumed this month
  – Collect and evaluate data
    ▪ Discussions
    ▪ E-Mails and other feedback
    ▪ PoC implementation
NTS4PTP
next steps

• Working on different documents for the NTP working group:
  – [1] a TL;DR/overview version of NTS4PTP (1-2 pages)
    ▪ Describes the current protocol structure and communication flow
    ▪ Key features and design decisions (+ reference to the sections in the requirement document)

    ▪ Further and detailed information about the key features and design decisions
    ▪ Discusses and compares alternatives for each property of the NTS4PTP protocol
    ▪ Contains a small vote and discussion section

➔ It is easier for you if you want to give some feedback, ideas or votes

• After this, I update the current draft document
Thank you for your attention!

Martin Langer
Physikalisch-Technische Bundesanstalt
Braunschweig, Germany

Rainer Bermbach
Ostfalia University of Applied Sciences,
Wolfenbüttel, Germany
NTS4PTP

Protocol Overview – Group-Based Approach

- Same procedure for every PTP instance of the group

Secured PTP messages using **group key**

- **Secured PTP Announce**
- **Secured PTP Sync + Follow_Up**
- **Secured PTP Delay_Req**
- **Secured PTP Delay_Resp**

Key Response contains:
- Group ID, security parameters, **group key**, validity period, etc.

Authenticated & encrypted TLS communication
- Group key-authenticated PTP communication

NSS-KE Server

PTP Instance

Secured PTP Network
NTS4PTP
Protocol Overview – Ticket-Based Approach

**Requester**
- Wants unicast connection
- Gets *unicast key* and encrypted *ticket*
- Secured PTP message (using *unicast key*) contains *ticket*

**NTS-KE Server**
- KE server generates *ticket key*
- Generates *unicast key* and encrypted *ticket*

**Grantor**
- Registers upfront and commits security parameters
- Gets *ticket key* to decrypt tickets
- Decrypts *ticket* (using *ticket key*) and extracts the containing *unicast key*