NTS4PTP

Network Time Security for the Precision Time Protocol

Update Report of the Draft

Martin Langer, Rainer Bermbach

IETF NTP working group, June 22, 2021
Agenda

• Goals and Features
• Protocol Overview
• Draft Status
NTS4PTP

Goals

• We need a security solution for PTP
  – PTPv2.1 provides an AUTHENTICATION TLV
  – The key management system is out of scope

• Idea: Using NTS as a key management system for PTP
  – Then we have one NTS-KE server, which supports NTP and PTP

• We want a solution for all PTP functionalities and modes
  – Not easy and very different to NTP
NTS4PTP

Features

- NTS4PTP defines two approaches:
  - Group-based approach (GrBA): for PTP multicast and mixed multicast/unicast
  - Ticket-based approach (TiBA): for PTP unicast only (scalable)

- We have extended the NTS-KE protocol to support PTP

- We have defined the NTS Time Server Registration (NTS-TSR) protocol
  - The communication between time server (PTP grantor) and NTS-KE server
  - Therefore, the NTS-KE server can run the NTS-KE and NTS-TSR protocol (depending on the ALPN)
    - Necessary to be able to distinguish messages
More features:

- Group- and E2E security
- Cyclic key update process
  - Without interruption of PTP communication
  - Simple group control

- PTP grantor and algorithm negotiation for unicast connections
NTS4PTP
Protocol Overview – Group-Based Approach

- Same procedure for every PTP instance of the group

Secured PTP messages using **group key**
NTS4PTP
Protocol Overview – Group-Based Approach

- Same procedure for every PTP instance of the group

![Diagram showing secured PTP messages and TLS communication](Image)

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

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

**TLS**
- PTP Key Request
- PTP Key Response

**NTS-KE Server**

**Secured PTP Network**

**PTP Instance**

**Authenticated & encrypted TLS communication**

**Group key-authenticated PTP communication**
NTS4PTP
Protocol Overview – Group-Based Approach

• Same procedure for every PTP instance of the group
NTS4PTP

Protocol Overview – Ticket-Based Approach

Requester wants unicast connection

Requester gets unicast key and encrypted ticket

Secured PTP message (using unicast key) contains ticket

KE server generates ticket key

PTP registration request

PTP registration response

KE server generates unicast key and encrypted ticket

Grantor registers upfront and commits security parameters

Grantor gets ticket key to decrypt tickets

Authenticated & encrypted TLS communication

Group key-authenticated PTP communication

Grantor decrypts ticket (using ticket key) and extracts the containing unicast key

Secured PTP Announce Request

Secured PTP Grant
## NTS4PTP

### Protocol Overview – Ticket-Based Approach

<table>
<thead>
<tr>
<th>PTP Requester</th>
<th>NTS-KE Server</th>
<th>PTP Grantor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requester wants unicast connection</td>
<td>KE server generates <strong>ticket key</strong></td>
<td>Grantor registers upfront and commits security parameters</td>
</tr>
<tr>
<td>Requester gets <strong>unicast key</strong> and encrypted <strong>ticket</strong></td>
<td>KE server generates <strong>unicast key</strong> and encrypted <strong>ticket</strong></td>
<td>Grantor gets <strong>ticket key</strong> to decrypt tickets</td>
</tr>
<tr>
<td>Secured PTP message (using <strong>unicast key</strong>) contains <strong>ticket</strong></td>
<td></td>
<td>Grantor decrypts <strong>ticket</strong> (using <strong>ticket key</strong>) and extracts the containing <strong>unicast key</strong></td>
</tr>
</tbody>
</table>

**Secure PTP message (using **unicast key**)**

- **Authentication & encrypted TLS communication**
- **Group key-authenticated PTP communication**
Protocol Overview – Ticket-Based Approach

Langer, Bermbach IETF NTP working group

KE server generates \textit{ticket key} and encrypted ticket

Requester wants unicast connection

Requester gets \textit{unicast key} and encrypted ticket

Secured PTP message (using \textit{unicast key}) contains ticket

KE server generates \textit{unicast key} and encrypted ticket

Secured PTP (using \textit{unicast key}) contains ticket

Grantor registers upfront and commits security parameters

Grantor gets \textit{ticket key} to decrypt tickets

Authenticated & encrypted TLS communication

Group key-authenticated PTP communication

Grantor decrypts ticket (using ticket key) and extracts the containing \textit{unicast key}
NTS4PTP
Protocol Overview – Ticket-Based Approach

<table>
<thead>
<tr>
<th>PTP Requester</th>
<th>KE server generates ticket key</th>
<th>PTP Grantor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requester wants unicast connection</td>
<td>KE server generates unicast key and encrypted ticket</td>
<td>Grantor registers upfront and commits security parameters</td>
</tr>
<tr>
<td>Requester gets unicast key and encrypted ticket</td>
<td>KE server generates unicast key and encrypted ticket</td>
<td>Grantor gets ticket key to decrypt tickets</td>
</tr>
<tr>
<td>Secured PTP message (using unicast key) contains ticket</td>
<td>KE server generates ticket key</td>
<td>TLS Authorized &amp; encrypted TLS communication</td>
</tr>
<tr>
<td>TLS PTP Key Request</td>
<td>TLS PTP Key Response</td>
<td>Secured PTP Group key-authenticated PTP communication</td>
</tr>
<tr>
<td>TLS PTP Registration Request</td>
<td>TLS PTP Registration Response</td>
<td>Grantor decrypts ticket (using ticket key) and extracts the containing unicast key</td>
</tr>
</tbody>
</table>

Langer, Bermbach
IETF NTP working group
NTS4PTP
Draft Status

• Current version: draft-langer-ntp-nts-for-ptp-01

• Next update in 6 to 8 weeks

• The following version contains many changes
  – NTS messages were simplified
  – Key rotation process has been optimized
  – Clarifications and text improvements
  – Preparation for PoC implementation underway
    ▪ possible integration into Linux PTP for initial tests
Thank you for your attention!

Martin Langer, Rainer Bermbach

Ostfalia University of Applied Sciences, Wolfenbüttel, Germany