Network Time Security

draft-ietf-ntp-cms-for-nts-messages-06
draft-ietf-ntp-network-time-security-14
draft-ietf-ntp-using-nts-for-ntp-05

Kristof Teichel, Dieter Sibold
NTS: WGLC Design Team Progress

• WGLC generated large amounts of feedback (too much for the two-man main team to manage)
• Led to creation of Design Team
Key Exchange

• IP fragmentation
  - NTS key exchange (MUST requirement in draft-ietf-ntp-using-nts-for-ntp-05) will cause IP fragmentation
    → potential problems with NAT devices
    → Negative implications on protocol security

• Considered alternatives
  - Applying DTLS for the key exchange
  - Time exchange always secured via NTS

<table>
<thead>
<tr>
<th>Key Exchange (KE)</th>
<th>Port KE</th>
<th>Port TE</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTS Custom</td>
<td>NTP-EF via 123/udp</td>
<td>123/udp</td>
</tr>
<tr>
<td>NTS Custom</td>
<td>NNN/tcp</td>
<td>123/udp</td>
</tr>
<tr>
<td>DTLS native</td>
<td>NNN/udp</td>
<td>123/udp</td>
</tr>
<tr>
<td>DTLS over NTP</td>
<td>123/udp</td>
<td>123/udp</td>
</tr>
</tbody>
</table>
Key Exchange (continued …)

• Issues to deal with for any KE candidate
  – How to avoid fragmentation on IP level?
  – Whether/how to deal with rate limitations and NTP port usage? (Assumed important)

<table>
<thead>
<tr>
<th>Port for KE</th>
<th>Adhere to usual NTP rate limitations?</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP 123</td>
<td>YES</td>
<td>• Maximum compatibility,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Possibly very (!) slow</td>
</tr>
<tr>
<td>UDP 123</td>
<td>NO</td>
<td>• Might not be accepted at certain NTP providers</td>
</tr>
<tr>
<td>UDP != 123 or TCP</td>
<td>NO</td>
<td>• Requires additional open port (might slow down rollout)</td>
</tr>
</tbody>
</table>
Key Exchange (continued …)

• Issues to deal with for any KE candidate
  – Under which conditions to allow usage of unauthenticated time stamps?
  – Whether/how to handle peer mode?
  – Whether/how to include authorization?
  – Requirement for two-way authentication?
  – How to ensure cryptographic algorithm agility (BCP 201)?
Questions about NTS Key Exchange

• Fewer overall exchanges?
• Fewer cryptographic operations?
• Seed refresh: to mention or not?
Other Agenda Items

• Improve handling of cipher suites (for MAC generation)
  • (draft-aanchal4-ntp-mac-00)
  • Already done in NTS: generalize from HMAC to MAC

• Discussion about Chicken-and-Egg problem

• Discussion about benefits/disadvantages of different overall security mechanisms

• Symmetry of message sizes in time sync exchange
Next steps

• Clarification of which KE is mandatory in NTS for NTP draft
• Consideration/inclusion of Daniel Franke’s proposal
• Specification of KE in NTS for NTP draft
• Related
  • Peer mode
  • Usage of unauthenticated timing information
• Consideration/inclusion of draft-aanchal4-ntp-mac-00
Next steps (continued …)

• New version of draft-ietf-ntp-using-nts-for-ntp
• WGLC right after IETF 97th (Seoul)
  • Also requires WGLC for generic NTS (!)
  • May be possible without CMS-4-NTS (depending on choice of key exchange mechanism)