IETF Hackathon: Network Time Security (NTS)

IETF 104
23-24 March, 2019
Prague
Hackathon Plan

• Integration of NTS into different NTP implementations
  • Based on draft-ietf-ntp-using-nts-for-ntp-17

• Verifying interoperability between various NTS implementations
## What got done

<table>
<thead>
<tr>
<th>IETF 104 Hackathon Results Overview</th>
<th>NTP NTS Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ostfalia Server</td>
</tr>
<tr>
<td>Implementation Status</td>
<td>Done</td>
</tr>
<tr>
<td><strong>NTP NTS Clients</strong></td>
<td></td>
</tr>
<tr>
<td>Ostfalia Client</td>
<td></td>
</tr>
<tr>
<td>Chrony Client</td>
<td></td>
</tr>
<tr>
<td>NTPSec Client</td>
<td></td>
</tr>
<tr>
<td>Netnod (Python) client</td>
<td></td>
</tr>
<tr>
<td>Netnod (Golang) (Malmö) client</td>
<td></td>
</tr>
<tr>
<td>NTF client (*)</td>
<td>In Progress</td>
</tr>
</tbody>
</table>

KE = Key Exchange worked  
NTP = authenticated NTP packets successfully exchanged

(*) NOTE: implementing draft-ietf-ntp-using-nts-for-ntp-11
What we did/learned

• Several bug fixes in the implementations

• Some issues with OpenSSL (bug in TLS key exporter function)

• Interoperability test was very successful

• No further problems in the NTS-draft discovered
Wrap Up

Team members:
- Karen O'Donoghue (ISOC)
- Dieter Sibold (PTB)
- Richard Welty (NTF)
- Martin Langer (Ostfalia University)
- Christer Weinigel (Netnod)
- Watson Ladd (Cloudflare)
- Aanchal Malhotra (Boston University, Cloudflare)
- Miroslav Lichvar (Red Hat) (remote)
- Hal Murray (NTPSec) (remote)
- Sanjeev Gupta (NTPSec) (remote)
- Gary Miller (NTPSec) (remote)
- Michael "MC" Cardell Widerkrantz (Malmö) (remote)
- Martin "cos" Samuelsson (Malmö) (remote)

NTP working group:
https://datatracker.ietf.org/wg/ntp

Involved documents:
draft-ietf-ntp-using-nts-for-ntp-17
RFC 5905 (NTPv4)
RFC 5297 (AES-SIV)
RFC 7822 (NTP EF)

Repositories:
https://gitlab.com/MLanger/nts
https://github.com/Netnod/nts-poc-python
https://github.com/wbl/nts-rust
https://github.com/mlichvar/chrony-nts
https://gitlab.com/NTPsec/ntpsec