IETF Hackathon: Network Time Security (NTS)

IETF 102
14-15 July, 2018
Montreal
Hackathon Plan

• Integration of NTS with different NTP implementation
  • draft-ietf-ntp-using-nts-for-ntp-12
  • draft-dansarie-nts-00

• Verifying interoperability between various NTS implementations
Team and Technology

Team members:

- **NTS-M (Martin)** - draft-ietf-ntp-using-nts-for-ntp-11 (C++)
- **NTS-D (Daniel)** - draft-ietf-ntp-using-nts-for-ntp-11 (Python)
- **NTS-S (Sweden)** - Malmö team - draft-dansarie-nts-00 (golang)
- **NTS-N (NTF)** - draft-ietf-ntp-using-nts-for-ntp-12 (NTPD)
- **NTS-O (Jean-Philippe)** - draft-ietf-ntp-using-nts-for-ntp-12 (OpenNTPD)

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

Involved documents:
- draft-ietf-ntp-using-nts-for-ntp-12
- draft-dansarie-nts-00
- RFC 5905 (NTPv4)
- RFC 5297 (AES-SIV)
- RFC 7822 (NTP EF)

Git repositories:
- https://github.com/dfoxfranke/nts-hackathon
- https://gitlab.com/MLanger/nts
- https://gitlab.com/MLanger/ntp
- https://github.com/beevik/ntp
- https://github.com/bifurcation/mint
- https://github.com/beevik/ntp
- TLS 1.3
- https://github.com/beevik/ntp
IETF Hackathon – Network Time Security (NTS)
# What got done

<table>
<thead>
<tr>
<th>Team</th>
<th>Draft</th>
<th>Language</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Martin</td>
<td>draft-ietf-ntp-using-nts-for-ntp-11/12</td>
<td>C++</td>
<td>Continuation of hackathon 101</td>
</tr>
<tr>
<td>Daniel Lavinia Lee</td>
<td>draft-ietf-ntp-using-nts-for-ntp-11/12</td>
<td>Python</td>
<td>Continuation of hackathon 101</td>
</tr>
<tr>
<td>Team Sweden</td>
<td>draft-dansarie-nts-00</td>
<td>Golang</td>
<td>NTP in FPGA</td>
</tr>
<tr>
<td>Network Time Foundation</td>
<td>draft-ietf-ntp-using-nts-for-ntp-12</td>
<td>C</td>
<td>Start of NTS integration in NTP’s reference implementation</td>
</tr>
<tr>
<td>Jean-Philippe Ouellet</td>
<td>draft-ietf-ntp-using-nts-for-ntp-12</td>
<td></td>
<td>Start of implementation work</td>
</tr>
<tr>
<td>(openNTPD)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## What we did/learned

<table>
<thead>
<tr>
<th>Client/server</th>
<th>Martin (Server)</th>
<th>Python (Server)</th>
<th>Team Sweden Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Martin (Client)</td>
<td>Key and time exchange</td>
<td>KE as demonstrated at 101 Hackathon</td>
<td>TLS 1.3 issues between golang package and openssl</td>
</tr>
<tr>
<td></td>
<td>Time exchange: drop of NTP mode 3 packets between Germany and Montreal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Python (Client)</td>
<td>KE and TE demonstrated at 101 Hackathon</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Team Sweden Client</td>
<td>TLS 1.3 issues between golang package and openssl</td>
<td></td>
<td>Key and time exchange</td>
</tr>
<tr>
<td>NTF (Client)</td>
<td>First phase of KE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IETF Hackathon – Network Time Security (NTS)
Wrap Up

- Interoperability tests are important
- The NOC is very helpful!
- Wireshark helps...