# 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

| IETF 104 Hackathon Results Overview | | | NTP NTS Servers | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Ostfalia Server | Chrony Server | NTPSec Server | Netnod (Python) Server | Netnod (Golang) (Malmö) Server | NTF Server (*) | Cloudflare NTS Server |
| | | Implementation Status | Done | Done | Done | Done | In Progress | In Progress | In Progress |
| NTP NTS Clients | Ostfalia Client | Done | KE, NTP | KE, NTP | KE, NTP | KE, NTP | | | |
| | Chrony Client | Done | KE, NTP | KE, NTP | KE, NTP | KE, NTP | | | |
| | NTPSec Client | Done | KE, NTP | KE, NTP | KE, NTP | KE, NTP | | | |
| | Netnod (Python) client | Done | KE,NTP | KE,NTP | KE, NTP | KE, NTP | | | |
| | Netnod (Golang) (Malmö) client | Done | KE | | | | | | |
| | NTF client (*) | In Progress | | | | | | | |

**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 (Cloudfare)
- 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