IETF 108 Hackathon

Network Time Security

July 20-24, 2020
Hackathon Plan

Primary Goal
• Interoperability tests between the current NTS implementations
  • Based on the latest draft version of NTS

Secondary Goals
• Advanced NTS tests (strict compliance of the NTS specification)
• Performance tests
Test Setup

- 14 NTS/NTP servers (in different countries)
  - California (USA), Germany, Netherlands, Singapore, Sweden

- 5 NTP-Implementations with NTS support
  - Chrony
  - Cloudflare NTS (cfnts)
  - Ostfalia NTP (ntp-o)
  - NTPsec
  - Python/FPGA
Results (1/3)

Interoperability Tests

• All implementations talk to each other

• Everyone is strict in what they send
  • ...but maybe not strict enough in what they accept (→ see Results 2/3)

• We still have issues with international connections
  • Some operators filtering the NTS-secured NTP packets
Results (2/3)

Advanced NTS Tests

• Miroslav Lichvar has written an NTS-KE testing tool
  • It checks the implementations for compliance with the NTS specification
  • https://github.com/mlichvar/ntske-test

• Many FAILs, but no serious problems
  • Some implementations tolerate (non-critical) errors, instead of aborting the processing
    ➔ several “bugs” are known or intentional accepted
    ➔ for backwards compatibility (e.g. TLS v1.2)
  • Few bugs were fixed during the hackathon
Advanced NTS Tests

Results:

- [https://docs.google.com/spreadsheets/d/1QjLjgVcv0dEnAS0sHWt8ZZSrbumvQA2gaSBF3fLuCLM/view](https://docs.google.com/spreadsheets/d/1QjLjgVcv0dEnAS0sHWt8ZZSrbumvQA2gaSBF3fLuCLM/view)
Results (3/3)

Performance Tests
• Based on the NTS-KE testing tool

• Up to 3300 NTS-KE sessions per second were achieved
  • Depends on the implementation and the hardware performance
Conclusion

• The Hackathon was successful!

• Automatic testing tools are very useful

• The interoperability is still good

• No issues in the NTS specification identified
Thanks to all team members and the organizers

- Team members:
  - Christer Weinigel
  - Denis Reilly
  - Dieter Siebold
  - Kai Heine (First timer @ IETF/Hackathon)
  - Karen O’Donoghue
  - Martin Langer
  - Miroslav Lichvar
  - Phil Roberts
  - Sanjeev Gupta
  - Watson Ladd

- Sources:
  - https://github.com/mlichvar/chrony.git
  - https://gitlab.com/NTPsec/ntpsec
  - https://github.com/Netnod/nts-poc-python
  - https://gitlab.com/MLanger/nts