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
  - https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp-28

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

Results (2/3)

Advanced NTS Tests

- Results:
  - https://docs.google.com/spreadsheets/d/1QjLjgVcvOdEnAS0sHWt8ZZSrbmvrQA2gaSBF3fLuCLM/view

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	**Server**	netmon2.dcs1.biz	ntp1.glypnod.com	ntp2.glypnod.com	ntpmon.dcs1.biz	nts-test.strangled.r	nts.ntp.se	nts.sth1.ntp.se	nts.sth2.ntp.se	nts1.time.nl	nts2-e.ostfalia.de	nts3-e.ostfalia.de	time.cloudflare.com	timemaster.evangr
2	**Server Implementation**	**ntpsec**	**ntpsec**	**ntpsec**	**ntpsec**	**chrony**	**Python/chrony**	**Python/FPGA**	**Python/FPGA**	**ntpsec**	**ntp-o**	**ntp-o**	**cloudflare nts**	**chrony**
3	TLSv1.3 connection	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
4	Rejection of TLSv1.2 connection	FAIL	PASS	PASS	PASS	FAIL	FAIL	PASS	PASS	PASS	PASS	PASS	PASS	FAIL
5	ALPN "ntske/1"	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
6	Rejection of unknown ALPN	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	PASS	PASS	FAIL	PASS	PASS	FAIL	PASS
7	Minimal valid request	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
8	Number of cookies	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	FAIL	PASS
9	Missing NEXT_PROTOCOL record	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	PASS	FAIL	PASS
10	Missing AEAD_ALGORITHM record	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	PASS	FAIL	PASS
11	Multiple NEXT_PROTOCOL records	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	PASS	FAIL	FAIL
12	Multiple AEAD_ALGORITHM records	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	PASS	FAIL	FAIL
13	Missing NEXT_PROTOCOL value	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	FAIL	FAIL	PASS
14	Missing AEAD_ALGORITHM value	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	FAIL	FAIL	PASS
15	Multiple NEXT_PROTOCOL values	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	FAIL	FAIL	PASS	PASS
16	Multiple AEAD_ALGORITHM values	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
17	Unknown NEXT_PROTOCOL value	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	FAIL	PASS	FAIL	FAIL
18	Unknown AEAD_ALGORITHM value	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	FAIL	PASS	FAIL	FAIL
19	Unknown SERVER_NEGOTIATION	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
20	Unknown PORT_NEGOTIATION	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
21	Unknown critical record	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	FAIL	FAIL	FAIL	FAIL
22	Unknown non-critical record	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
23	Missing END_OF_MESSAGE	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	FAIL	FAIL	FAIL	PASS
24	Slow request	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	FAIL	FAIL	PASS	PASS
25	Long request	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS

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