IETF 101 Hackathon: Network Time Security (NTS)

Martin Langer (Ostfalia), Dieter Sibold (PTB),
Daniel Fox Franke, Richard Welty

IETF 101
17-18 March, 2018
London

Hackathon Plan

- **Goal:**
  - Find remaining issues in the NTS draft (draft-ietf-ntp-using-nts-for-ntp-11)

- **How can we achieve this?**
  - Interoperability test with two independent *Proof of Concept* (PoC) implementations of NTS

State of the Implementations

- **PoC 1 (by Martin Langer):**
  - Based on C++14
  - For multiple platforms (Windows (x86), Linux (x86/ARM))
  - 90%-95% completed
    - NTS Implementation is functional
      - Error/Warning records (NTS KE) still need to be added
    - Applies an NTPv4 implementation of Ostfalia Univ. as a testbed
    - In-depth tests and code reviews are still needed

State of the Implementations

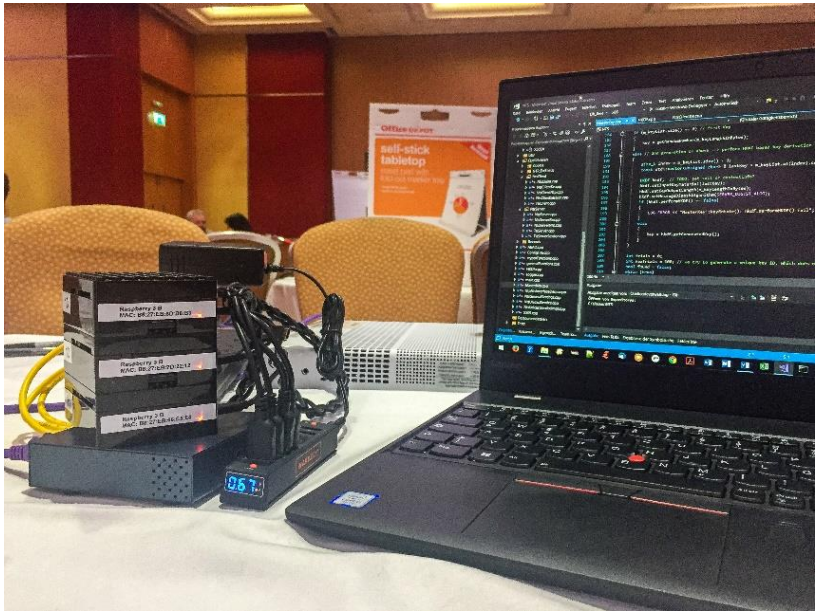
- **PoC 2 (by Daniel Fox Franke):**
  - Based on Phyton
  - Only for test purpose and proof of concept
    - NTS KE (over TLS) finished
    - NTP message exchange not completed
      - Client side is finished
      - Server side is still in progress
  - Very first software test was on the Hackathon

State of the Implementations

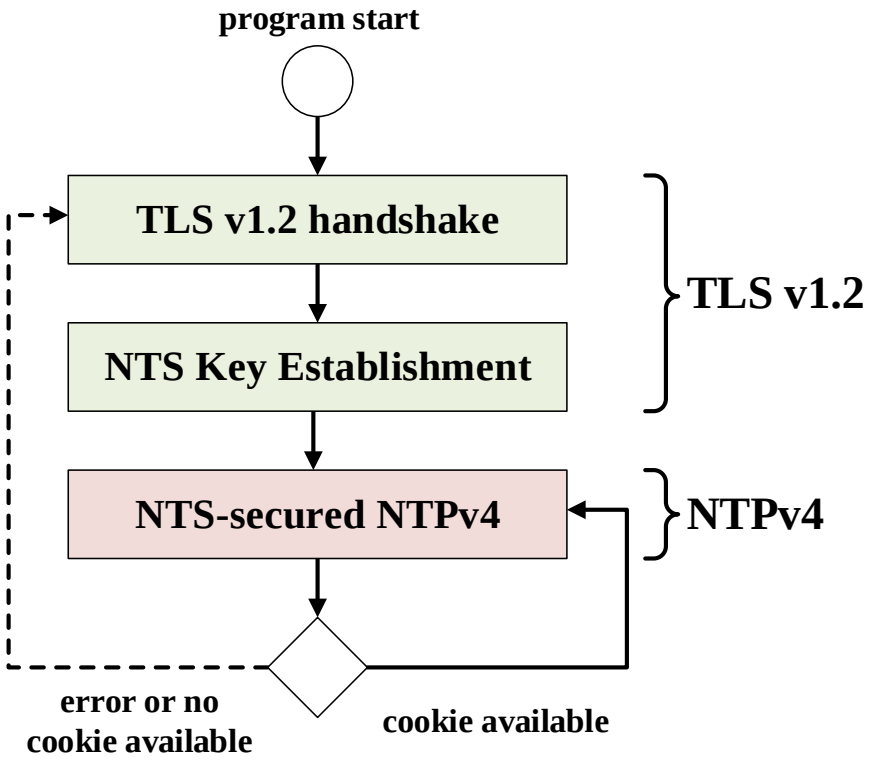
- **PoC 3 (by 3 students of the Ostfalia University):**
  - Based on C++11
  - 60-70% completed
    - Currently not ready for test
    - Planned completion: mid 2018

What got done

- **Setup for interoperability test (connection over Internet)**



Protocol Phases to be Tested



What got done

- **First test scenario (Hackathon)**
  - NTS client (PoC 2) against NTS server (PoC 1)

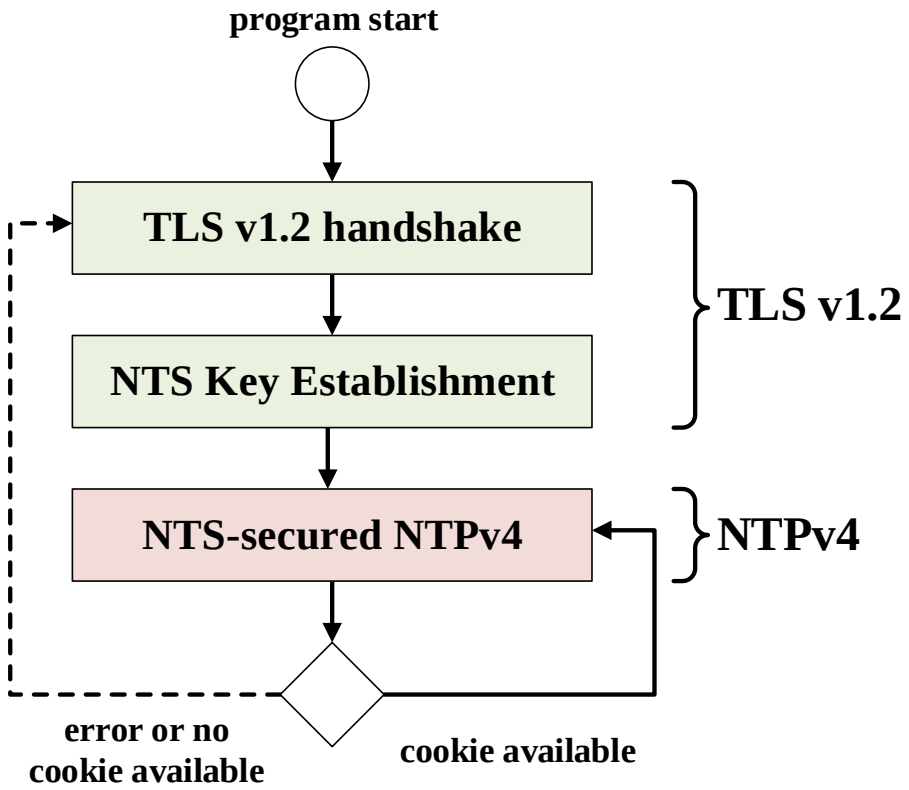
- **Test results**
  - NTS KE was successful
  - NTS time exchange revealed that PoC 1 misinterpreted the handling of NTS cookies by the server
  - NTS time exchanged verified successfully after correction of PoC 1 in accordance to the draft

What got done

- **Second test scenario (Code Launch on Tuesday)**
  - NTS client (PoC 1) against NTS server (PoC 2)

- **Test results**
  - NTS KE was successful
  - NTS time exchange is not yet ready for test

Overview of Results



TLS v1.2

PoC1 (Client) → PoC2 (Server) = **OK**
PoC2 (Client) → PoC1 (Server) = **OK**

PoC1 (Client) → PoC2 (Server) = **OK**
PoC2 (Client) → PoC1 (Server) = **OK**

NTPv4

PoC1 (Client) → PoC2 (Server) = test pending
PoC2 (Client) → PoC1 (Server) = **OK**

What we learned

- Interoperability test is pretty important to find hidden issues within specifications
- We know the current draft works perfectly

- **What we have to do now?**
  - Fine-tuning on some protocol points
  - Complete the tests

Wrap Up

Team members:

Karen O'Donoghue

First timers @ IETF/Hackathon:

Daniel Fox Franke

Richard Welty

Dieter Sibold

Martin Langer

NTP working group:

https://datatracker.ietf.org/wg/ntp

Involved documents:

draft-ietf-ntp-using-nts-for-ntp-11

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