Interop overview

IETF 111, LAKE WG, July 29th, 2021

Implementations

- 7 available and tested implementations – Aligned with EDHOC **v -06**
  - Marco Tiloca (RISE): Java (*Eclipse Californium)*
  - Timothy Claeys (INRIA): Python (*py-edhoc*) ; C
  - Christian Amsüss: Python (*aiocoap*)
    - Building on the *py-edhoc* from Timothy
  - Peter van der Stok: C
  - Stefan Hristozov (Fraunhofer): C
  - Lidia Pocero (ISI): Contiki-NG

- Further implementations to test
  - Michel Veillette
  - Michael Richardson
  - Inria (Rust/hacspec)

Implementations – Worth noting

- Stefan Hristozov (Fraunhofer): C
  - Experimental evaluation published in [1], covering four HW architectures
  - Results presented also at the LAKE interim meeting in April [2]

- Lidia Pocero (ISI): Contiki-NG
  - Run and tested over a Zoul device (CC2538 chipset)
  - Setup: RPL over an IPv6 mesh network

[1] https://arxiv.org/pdf/2103.13832.pdf
[2] https://datatracker.ietf.org/doc/slides-interim-2021-lake-02-sessa-uedhoc-performance-evaluation/

Interop tests since IETF 110

- Spontaneous bilateral tests

- Interop event on April 14, 2021 – Version -05 of the draft
  - Tested implementations: Marco, Peter, Christian, Timothy (C-based), Stefan
  - Reported at the LAKE interim meeting on April 22

- Interop event on May 18, 2021 – Version -06 of the draft
  - Tested implementations: Marco, Christian, Lidia
  - Reported at the LAKE interim meeting on June 1

- About 10 attendees at each interop event

Interop tests since IETF 110

- Detailed notes and results at:
  - https://drive.google.com/drive/folders/1gYHR0DQt7--K3y4PWXWVJZ203pKl3_3k
  - Including report template and a spreadsheet with supported/tested features

- Tested configurations – (Ciphersuite, Authentication Method, Credential Type)
  - 3 implementation pairs: (2, 3, kid)
  - 2 implementation pairs: (0, 0, x5t)
  - 1 implementation pair:
    - (0, 3, kid) ; (0, 3, x5t) ; (0, 0, kid)
    - (2, 0/1/2/3, kid) ; (2, 0/1/2/3, x5chain) ; (2, 3, x5t)
    - (3, 0/1/2/3, kid) ; (3, 0/1/2/3, x5chain)

Interop tests since IETF 110

- Detailed notes and results at:
  - https://drive.google.com/drive/folders/1gYHR0DQt7--K3y4PWXWVJZ203pKl3_3k
  - Including report template and a spreadsheet with supported/tested features

- 6 tested implementation pairs – 3 in both directions (*)
  - Marco with:
    - Peter
    - Stefan
    - Lidia (*)
    - Christian (*)
  - Timothy with Christian (*)
  - Lidia with Christian

Next steps

- Need to align implementations with version -08 of the draft
  - Connection identifiers can be binary strings or integers
  - New way of computing TH2 and TH3
  - New interface for the EDHOC-Exporter
  - Thinking of CoAP, Null byte prepended to message_1
  - …

- Run more interop tests during the autumn
  - First, repeat the tests for protocol completion and OSCORE Security Context derivation
  - Good to test also the use of message_4, EAD_x and error messages

Thank you!