EDHOC-PSK Interoperability Testing

Elsa López-Pérez (Inria)
Francisco López-Gómez (UMU)

What is EDHOC?

- Ephemeral Diffie Hellman Over COSE (EDHOC) is a lightweight authenticated key exchange protocol.
- There is an ongoing effort to define and standardize a new authentication method based on Pre Shared Keys (PSK)
- EDHOC-PSK is defined in https://datatracker.ietf.org/doc/draft-ietf-lake-edhoc-psk/

Starting point

💻Two implementations:

1. University of Murcia (UMU) implementation: C code based on uOSCORE-uEDHOC 3.0.5.
   https://gitlab.com/franciscolopezg/edhoc-psk-interop-ietf123
2. Inria Implementation: Rust code
   https://github.com/ElsaLopez133/lakers/tree/PSK2-coap-inter-test

Test being made on PCs for simplicity, but also working in constrained devices.

Work done

1. Updating both implementations to the last version of the draft (04).
2. Inconsistencies detected in the draft regarding the use of CRED_PSK for key and derivation.

There is a need to specify two different terms: CRED_PSK and PSK

PRK_4e3m	EDHOC_Extract(SALT_4e3m, **PSK**)
TH_4	H(TH_3, ID_CRED_PSK, PLAINTEXT_3B, **CRED_PSK**)
external_aad in CIPHERTEXT_3B	<< ID_CRED_PSK, TH_3, **CRED_PSK** >>

3. UMU implementation now compliant with RFC9668.

Results

- ✅Interoperability achieved in both communication directions.
- ❌Need to update the draft to properly define credentials and keys, and include identities in credentials

✅INTEROPERABILITY ACHIEVED

UMU’s output when running as **Responder**:

```
Message 4  (size 9):
        48 FF 5B A5 2C E8 D1 6C 13
CoAP reply sent!
PRK_out (size 32):
        53 F2 72 7B B1 C1 59 05 51 97 C1 35 44 9C 0B FC
        E5 17 1B 0B A7 E3 18 CC 00 A1 39 E2 14 29 24 5F
```

```
PRK: (size 32):
        53 F2 72 7B B1 C1 59 05 51 97 C1 35 44 9C 0B FC
        E5 17 1B 0B A7 E3 18 CC 00 A1 39 E2 14 29 24 5F
prk_exporter (size 32):
        65 A7 CA D6 75 FE 3F 99 25 49 BE 5D F8 09 31 BA
        29 B8 12 D2 BC 18 34 A5 6D E0 8C 1D 69 3F CA C7
```

INRIA’s output when running as **Initiator**:

```
---------END-----------

EDHOC exchange successfully completed
PRK_out: [53, f2, 72, 7b, b1, c1, 59, 05, 51, 97, c1, 35, 44, 9c, 0b, fc, e5, 17, 1b, 0b, a7, e3, 18, cc, 00, a1
, 39, e2, 14, 29, 24, 5f]
PRK_out after key update: [4e, 40, 6d, ab, d9, 9e, 73, 3c, c8, bb, c1, d4, eb, 6f, 07, a6, 75, b1, 7a, 19, 00, a
8, f3, 4c, 9f, 11, 16, fe, fb, 16, a6, 2b]?
Handshake completed
```

❌Need to update the draft

- The confusion with CRED_PSK and PSK during the implementation, plus the vulnerability against selfie attacks led to a discussion on **how to properly define the credential and the key.**
- There will be some updates on the draft:
  - update of CRED_PSK: there will be two credentials CRED_I and CRED_R
  - both CRED_I and CRED_R have the same raw key
  - There is a single ID_CRED_PSK to identify both CRED_I and CRED_R

New interoperability testing will be needed