EDHOC Rekey

Rafael Marín López (UMU)

John Preuß Mattsson (Ericsson)

Motivation

- During the definition of the EAP method EAP-EDHOC, where EDHOC is performed as authentication protocol, we considered to provide resumption capabilities to the EAP method.
- Resumption consists of:
  - Message sizes in the protocol.
  - Less asymetric operations in the protocol
  - External things like fetching credentials from a database, revocation, path validation,
- If EDHOC had a rekey mechanism this can be used directly in the EAP method (or any other application).

Options for the rekey

1. Re-run EDHOC: EDHOC is lightweight enough. Just redo full EDHOC. (similar to full handshake in TLS)
2. Use PSK with ECDHE (similar to psk_dhe_ke in TLS and IKEv2 SA rekey, recommended for IPsec SA rekey)
3. Use PSK with exchanged random values (similar to psk_ke in TLS; possible in IPsec SA rekey)
4. Derive from PSK without new randomness (similar to key update in TLS)

Discussion of option 2 and 3

- Both 2. and 3. eliminate “External things like fetching credentials from a database, revocation, path validation”
- Rerunning full EDHOC requires 3 asymmetric operations. 2. requires 1 and 3. requires 0 asymmetric operation.
- 2. provides significantly better security. 3. should only be allowed for limited time resumption.
- Reuse of PSK identifiers is a major privacy problem. Enables tracking and fingerprinting. Needs to be solved.
- Rekeying could be specified as a new EDHOC method similar to TLS resumption.
- Would EDHOC with External PSK authentication be useful for other things than rekeying?

Conclusion

- We could try to define this in EAP-EDHOC within EMU WG but we believe it is better if EDHOC rekey is studied and designed in LAKE WG

- One suggestion:
  - Register 2. as the new EDHOC Method 4 that:
    - Remove ID_CRED_I and ID_CRED_R. Add ID_PSK to message_1
    - Include PSK in key derivation
    - Define new label for derivation of new PSK identifier.
    - Define new label for derivation of new PSK (when method 0,1,2,3 was used).