Key exchange for OSCORE

Göran Selander, Ericsson

Background

- OSCORE is adopted by various WGs and SDOs
- OSCORE depends on a pre-established strong Master Secret. Two alternatives are defined:
  - Pre-shared key
  - OSCORE profile of ACE (draft-ietf-ace-oscore-profile)
- A key exchange protocol is needed for use cases which require forward secrecy.

Paths for standardization

A. OSCORE profile of (D)TLS 1.3 handshake at application layer. Building blocks:
   - coDTLS: draft-schmertmann-dice-codtls
   - TLS-OSCORE: draft-mattsson-ace-tls-oscore
   - ATLS (mailing list)

B. Compact key exchange protocol built on CBOR and COSE
   - EDHOC: draft-selander-ace-cose-ecdhe

Comparison

A.

- SIGMA-I implemented in TLS 1.3 data structures
- Need adaptation for keying OSCORE:
  - negotiation of Sender/Recipient ID
  - derivation of Master Secret
- Thouroughly analysed

B.

- SIGMA-I implemented in CBOR, COSE and CoAP
  - reuse of OSCORE primitives
- Simpler protocol, limited functionality
- Smaller messages
- Formal verification in progress

Example of bytes and messages

	TLS – PSK +DH		TLS -- DH		EDHOC – PSK+DH		EDHOC - DH	
	Bytes	75	Bytes	75	Bytes	75	Bytes	75
Message #1	142	2	107	2	67	1	65	1
Message #2	135	2	264	4	66	1	173	3
Message #3	51	1	167	3	19	1	123	2
Total	328	5	538	9	152	3	361	6

The TLS figures exclude
OSCORE session identifiers.

Discussion

- EDHOC has lower message overhead with associated performance gain
- EDHOC reuses the same primitives as OSCORE enabling a low footprint
- Security-analysis-catch-22: To get more researchers interested in making security analysis, the IETF needs to show intent to progress this
- Approval can be conditioned on formal analysis and found issues resolved.
- What are the consequences of not standardizing a lightweight key exchange protocol?