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
   • Thoroughly 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

<table>
<thead>
<tr>
<th></th>
<th>TLS – PSK +DH</th>
<th>TLS -- DH</th>
<th>EDHOC – PSK+DH</th>
<th>EDHOC - DH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bytes</td>
<td>Bytes</td>
<td>Bytes</td>
<td>Bytes</td>
</tr>
<tr>
<td></td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>75</td>
</tr>
<tr>
<td>Message #1</td>
<td>142</td>
<td>2</td>
<td>107</td>
<td>2</td>
</tr>
<tr>
<td>Message #2</td>
<td>135</td>
<td>2</td>
<td>264</td>
<td>4</td>
</tr>
<tr>
<td>Message #3</td>
<td>51</td>
<td>1</td>
<td>167</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>328</td>
<td>5</td>
<td>538</td>
<td>9</td>
</tr>
</tbody>
</table>

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?