Comparison of CoAP Security Protocols

draft-ietf-lwig-security-protocol-comparison-03

LWIG

Prague

IETF 104

March 2019

draft-ietf-lwig-security-protocol-comparison-03

- **Changes between -01 and -02**
  - Updated based on changes in draft-ietf-tls-dtls13-30 that defined a single DTLSCiphertext structure.
    - Earlier versions had DTLSCiphertext and DTLSShortCiphertext.
- **Changes between -02 and -03**
  - Added message sizes for key exchange protocols. This has been the most requested addition since before version -00.
    - TLS 1.3 https://tools.ietf.org/html/rfc8446
    - DTLS 1.3 https://tools.ietf.org/html/draft-ietf-tls-dtls13-31
    - EDHOC https://tools.ietf.org/html/draft-selander-ace-cose-ecdhe-13
  - Some reformulations in the summary of application data .

Table of Contents

Assumptions

- **Message sizes for TLS 1.3, DTLS 1.3, and EDHOC are based on the following assumptions**
  - Minimum number of algorithms and cipher suites offered
  - Curve25519, ECDSA with P-256, AES-CCM_8, SHA-256
  - Length of key identifiers: 1 bytes
  - Length of connection identifiers: 1 byte
  - (D)TLS RPK with point compression (saves 32 bytes)
    - Specified but not implemented.
  - Only mandatory (D)TLS extensions, except for connection ID
  - No DTLS handshake message fragmentation

Lots of information

EDHOC

```
plaintext = <<
  h'a1',
  h'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d
    1e1f202122232425262728292a2b2c2d2e2f303132333435363738393a3b
    3c3d3e3f'
>>

message_2 = (
  h'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d
    1e1f',
  h'c4',
  h'000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d
    1e1f202122232425262728292a2b2c2d2e2f303132333435363738393a3b
    3c3d3e3f404142434445464748494a4b'
)

message_2 (114 bytes):
58 20 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11
12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 41 C4 58 51 00 01
02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15
16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29
2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D
3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B
```

(D)TLS RPK

```
0x30 // Sequence
0x59 // Size 89

0x30 // Sequence
0x13 // Size 19
0x06 0x07 0x2A 0x86 0x48 0xCE 0x3D 0x02 0x01
     // OID 1.2.840.10045.2.1 (ecPublicKey)
0x06 0x08 0x2A 0x86 0x48 0xCE 0x3D 0x03 0x01 0x07
     // OID 1.2.840.10045.3.1.7 (secp256r1)

0x03 // Bit string
0x42 // Size 66
0x00 // Unused bits 0
0x03 // Compressed
...... 32 bytes X
```

DTLS 1.3

```
Record Header - DTLSPlaintext (13 bytes):
16 fe fd EE EE SS SS SS SS SS SS LL LL

  Handshake Header - Client Hello (10 bytes):
  01 LL LL LL SS SS 00 00 00 LL LL LL

    Legacy Version (2 bytes):
    fe fd

    Client Random (32 bytes):
    00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
    16 17 18 19 1a 1b 1c 1d 1e 1f

    Legacy Session ID (1 bytes):
    00

    Legacy Cookie (1 bytes):
    00

    Cipher Suites (TLS_AES_128_CCM_8_SHA256) (4 bytes):
    00 02 13 05

    Compression Methods (null) (2 bytes):
    01 00

    Extensions Length (2 bytes):
    LL LL

      Extension - Supported Groups (x25519) (8 bytes):
      00 0a 00 04 00 02 00 1d

      Extension - Signature Algorithms (ecdsa_secp256r1_sha256)
      (8 bytes):
      00 0d 00 04 00 02 08 07

      Extension - Key Share (42 bytes):
      00 33 00 26 00 24 00 1d 00 20
      00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
      16 17 18 19 1a 1b 1c 1d 1e 1f

      Extension - Supported Versions (1.3) (7 bytes):
      00 2b 00 03 02 03 04

      Extension - Client Certificate Type (Raw Public Key) (6 bytes):
      00 13 00 01 01 02
```

Without Connection ID

Flight	#1	#2	#3	Total
DTLS 1.3 RPK + ECDHE	144	364	212	722
DTLS 1.3 PSK + ECDHE	178	183	56	417
DTLS 1.3 PSK	128	143	56	327
TLS 1.3 RPK + ECDHE	129	322	194	645
TLS 1.3 PSK + ECDHE	163	157	50	370
TLS 1.3 PSK	113	117	50	280

Figure 2: Comparison of message sizes in bytes without Connection ID

With Connection ID

Flight	#1	#2	#3	Total
DTLS 1.3 RPK + ECDHE	150	373	213	736
DTLS 1.3 Cached X.509/RPK + ECDHE	182	347	213	742
DTLS 1.3 PSK + ECDHE	184	190	57	431
DTLS 1.3 PSK	134	150	57	341
EDHOC RPK + ECDHE	39	114	80	233
EDHOC PSK + ECDHE	41	45	11	97

Figure 1: Comparison of message sizes in bytes with Connection ID

What's next?

- How would the group like to see the key exchange (handshake) information structured?
- What are the right use cases to compare, curent work was inspired by 6TiSCH
  - Key exchange and OSCORE over multi-hop Multi-hop network.
- What would the working group like to be added in future versions?
  - TLS 1.2 handshake https://tools.ietf.org/html/rfc5246
  - DTLS 1.2 handshake https://tools.ietf.org/html/rfc6347
  - Compact TLS 1.3 https://tools.ietf.org/html/draft-rescorla-tls-ctls
  - TLS Handshake in CBOR https://tools.ietf.org/html/draft-schaad-ace-tls-cbor-handshake
  - Application-Layer TLS https://tools.ietf.org/html/draft-friel-tls-atls
  - TLS Certificate Compression https://tools.ietf.org/html/draft-ietf-tls-certificate-compression
  - Group OSCORE https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm