ERICSSON

OVERHEAD OF COAP SECURITY PROTOCOLS

IETF100 LWIG, NOV 15 2017

DRAFT-MATTSSON-CORE-SECURITY-OVERHEAD-02

OVERVIEW

- draft-mattsson-core-security-overhead analyzes per-packet overhead for different security protocols used to secure CoAP.
  - DTLS 1.2 and DTLS 1.3 (ietf-tls-dtls13)
  - TLS 1.2 and TLS 1.3 (ietf-tls-tls13)
  - OSCORE (ietf-core-object-security)
- DTLS and TLS are analyzed with and without compression.
  - 6LoWPAN-GHC (RFC7400) and raza-6lo-compressed-dtls
- DTLS is analyzed with and without Connection ID
  - rescorla-tls-dtls-connection-id
- Analyzes “record layer”, not handshake.

Sequence Number	'05'	'1005'	'100005'
DTLS 1.2	29	29	29
DTLS 1.3	21	21	21
TLS 1.2	21	21	21
TLS 1.3	21	21	21
DTLS 1.2 (Raza)	13	13	14
DTLS 1.3 (Raza)	13	13	14
DTLS 1.2 (GHC)	16	16	17
DTLS 1.3 (GHC)	14	14	15
TLS 1.2 (GHC)	17	18	19
TLS 1.3 (GHC)	17	18	19
OSCORE Request	13	14	15
OSCORE Response	11	11	11

Figure 1: Overhead as a function of sequence number (Connection/Sender ID = '')

TLS 1.2 ⇒ DTLS 1.2 ⇒ DTLS 1.3

```
Content type:
17
Version:
03 03

Length:
00 16
Nonce:
00 00 00 00 00 00 00 05
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

TLS 1.2 (21 bytes overhead)
```

```
Content type:
17
Version:
fe fd
Epoch:
00 01
Sequence number:
00 00 00 00 00 05
Length:
00 16
Nonce:
00 00 00 00 00 00 00 05
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

DTLS 1.2 (29 bytes overhead)
```

```
Content type:
17
Version:
fe fd
Epoch:
00 01
Sequence number:
00 00 00 00 00 05
Length:
00 16

Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

DTLS 1.2 (21 bytes overhead)
```

- DTLS 1.2 has large overhead. DTLS 1.3 and TLS have less (but nor small) overhead.

Sequence Number	'05'	'1005'	'100005'
DTLS 1.2	29	29	29
DTLS 1.3	21	21	21
TLS 1.2	21	21	21
TLS 1.3	21	21	21
DTLS 1.2 (Raza)	13	13	14
DTLS 1.3 (Raza)	13	13	14
DTLS 1.2 (GHC)	16	16	17
DTLS 1.3 (GHC)	14	14	15
TLS 1.2 (GHC)	17	18	19
TLS 1.3 (GHC)	17	18	19
OSCORE Request	13	14	15
OSCORE Response	11	11	11

Figure 1: Overhead as a function of sequence number (Connection/Sender ID = '')

COMPRESSED TLS AND DTLS

- Both methods provides very good compression. raza-6lo-compressed-dtls achieves slightly better compression but requires state. GHC is stateless but provides slightly worse compression.
- 6LoWPAN-GHC is generic and can in addition to DTLS 1.2 handle DTLS 1.3, TLS 1.2, TLS 1.3, and DTLS with Connection ID.
  - GHC works very well for DTLS 1.3 as the version number is the same as in DTLS 1.2.
  - The compression of TLS is not as good as the compression of DTLS (as the static dictionary is more or less a DTLS record layer).
- raza-6lo-compressed-dtls cannot handle DTLS with Connection ID or TLS, all extensions requires an updated mechanism.
- The sequence number '01' used in [RFC7400], Figure 15 gives an exceptionally small overhead that is not representative.
- The header compression is not available when (D)TLS is exchanged over transports that do not use 6LoWPAN together with 6LoWPAN-GHC.

Sequence Number	'05'	'1005'	'100005'
DTLS 1.2	29	29	29
DTLS 1.3	21	21	21
TLS 1.2	21	21	21
TLS 1.3	21	21	21
DTLS 1.2 (Raza)	13	13	14
DTLS 1.3 (Raza)	13	13	14
DTLS 1.2 (GHC)	16	16	17
DTLS 1.3 (GHC)	14	14	15
TLS 1.2 (GHC)	17	18	19
TLS 1.3 (GHC)	17	18	19
OSCORE Request	13	14	15
OSCORE Response	11	11	11

Figure 1: Overhead as a function of sequence number (Connection/Sender ID = '')

OSCORE

```
OSCORE Request (13 bytes overhead)

CoAP Option Delta and Length
92
Option Value:
09 05
Payload Marker
ff
Ciphertext (incl. encrypted code):
ec ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9
```

```
OSCORE Response (11 bytes overhead)

CoAP Option Delta and Length
90
Option Value:
-
Payload Marker
ff
Ciphertext (incl. encrypted code):
ec ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9
```

- OSCORE has smaller overhead than compressed (D)TLS, and this small overhead is achieved even on deployments without 6LoWPAN or 6LoWPAN without DTLS compression.
- OSCORE is lightweight because it makes use of some excellent features in CoAP, CBOR, and COSE.

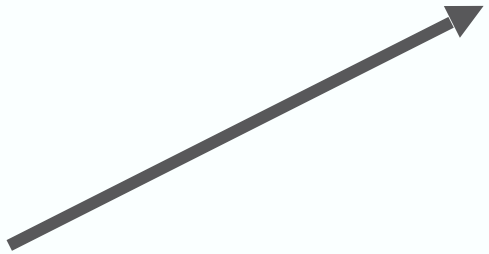
CONNECTION ID / SENDER ID

Connection/Sender ID	''	'42'	'4002'
DTLS 1.2	29	30	31
DTLS 1.3	21	22	23
DTLS 1.2 (GHC)	16	17	18
DTLS 1.3 (GHC)	14	15	16
OSCORE Request	13	14	15
OSCORE Response	11	11	11

Figure 2: Overhead as a function of Connection/Sender ID (Sequence Number = '05')

CONNECTION ID COMPRESSION

```
Content type:
17
Version:
fe fd
Epoch:
00 01
Sequence number:
00 00 00 00 00 05
Connection ID:
42
Length:
00 0e
```



```
Compressed Header and Nonce:
b0 c3 12 05 42 00 0e
```

```
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

DTLS 1.3 (22 bytes overhead).
```

```
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

DTLS 1.3 with 6LoWPAN-GHC (15 bytes overhead).
```

- 6LoWPAN-GHC (RFC7400) handles Connection ID optimally.

ERICSSON