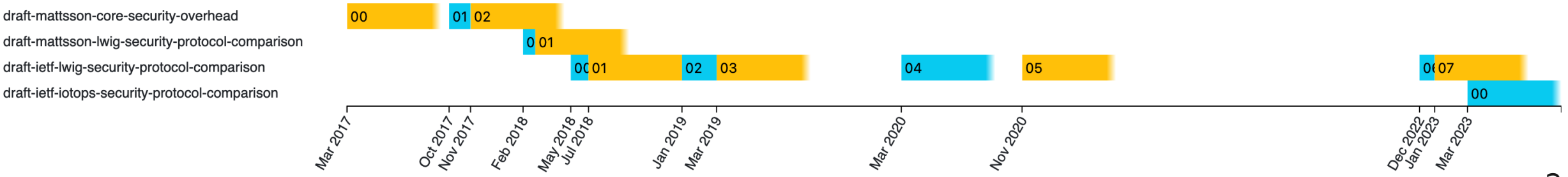
Comparison of CoAP Security Protocols

draft-ietf-iotops-security-protocol-comparison-00

draft-ietf-iotops-security-protocol-comparison-00

- The document analyzes and compares the sizes of key exchange flights and the per-packet message size overheads when using different security protocols to secure CoAP.
- The analyzed security protocols are DTLS 1.2, DTLS 1.3, TLS 1.2, TLS 1.3, cTLS, EDHOC, OSCORE, and Group OSCORE. The DTLS and TLS record layers are analyzed with and without 6LoWPAN-GHC compression.
  - No discussions regarding security or privacy.
  - Just message sizes for various configurations.
  - Some explanation of results.
- Discussed quite much in CORE and LWIG. Adopted in LWIG. LWIG rough agreement on content. Waited with updates until the protocols were more stable.



draft-ietf-iotops-security-protocol-comparison-00

Flight	#1	#2	#3	Total
DTLS 1.3 - RPKs, ECDHE	185	454	255	894
DTLS 1.3 - Compressed RPKs, ECDHE	185	422	223	830
DTLS 1.3 - Cached RPK, PRK, ECDHE	224	402	255	881
DTLS 1.3 - Cached X.509, RPK, ECDHE	218	396	255	869
DTLS 1.3 - PSK, ECDHE	219	226	56	501
DTLS 1.3 - PSK	136	153	56	345
EDHOC - X.509s, Signature, x5t, ECDHE	37	115	90	242
EDHOC - RPKs, Signature, kid, ECDHE	37	102	77	216
EDHOC - X.509s, Static DH, x5t, ECDHE	37	58	33	128
EDHOC - RPKs, Static DH, kid, ECDHE	37	45	19	101

Figure 1: Comparison of message sizes in bytes with CCM_8, P-256, and ECDSA and with Connection ID

draft-ietf-iotops-security-protocol-comparison-00

Flight	#1	#2	#3	Total
DTLS 1.3 - RPKs, ECDHE	179	447	254	880
DTLS 1.3 - PSK, ECDHE	213	219	55	487
DTLS 1.3 - PSK	130	146	55	331
TLS 1.3 - RPKs, ECDHE	162	394	233	789
TLS 1.3 - PSK, ECDHE	196	190	50	436
TLS 1.3 - PSK	113	117	50	280
cTLS - X.509s by reference, ECDHE	104	195	96	395
cTLS - PSK, ECDHE	105	119	20	226
cTLS - PSK	40	58	20	118

Figure 2: Comparison of message sizes in bytes with CCM_8, secp256r1, and ecdsa_secp256r1_sha256 or PSK and without Connection ID

draft-ietf-iotops-security-protocol-comparison-00

Flight	#1	#2	#3	Total
DTLS 1.3 - RPKs, ECDHE	146	360	200	706
DTLS 1.3 - PSK, ECDHE	180	186	55	421
DTLS 1.3 - PSK	130	146	55	331
TLS 1.3 - RPKs, ECDHE	129	307	179	615
TLS 1.3 - PSK, ECDHE	163	157	50	370
TLS 1.3 - PSK	113	117	50	280
cTLS - X.509s by reference, ECDHE	71	155	89	315
cTLS - PSK, ECDHE	72	86	20	178
cTLS - PSK	40	58	20	118

Figure 3: Comparison of message sizes in bytes with CCM_8, x25519, and ed25519 or PSK and without Connection ID

draft-ietf-iotops-security-protocol-comparison-00

Sequence Number	'05'	'1005'	'100005'
DTLS 1.2	29	29	29
DTLS 1.3	11	11	11
DTLS 1.2 (GHC)	16	16	16
DTLS 1.3 (GHC)	12	12	12
TLS 1.2	21	21	21
TLS 1.3	14	14	14
TLS 1.2 (GHC)	17	18	19
TLS 1.3 (GHC)	15	16	17
OSCORE request	13	14	15
OSCORE response	11	11	11
Group OSCORE pairwise request	14	15	16
Group OSCORE pairwise response	11	11	11

draft-ietf-iotops-security-protocol-comparison-00

Connection/Sender ID	''	'42'	'4002'
DTLS 1.2	29	30	31
DTLS 1.3	11	12	13
DTLS 1.2 (GHC)	16	17	18
DTLS 1.3 (GHC)	12	13	14
OSCORE request	13	14	15
OSCORE response	11	11	11
Group OSCORE pairwise request	14	15	16
Group OSCORE pairwise response	11	13	14

Figure 6: Overhead (8 bytes ICV) in bytes as a function of Connection/Sender ID (Sequence Number = '05')

draft-ietf-iotops-security-protocol-comparison-00

Protocol	Overhead	Overhead (GHC)
DTLS 1.2	21	8
DTLS 1.3	3	4
TLS 1.2	13	9
TLS 1.3	6	7
OSCORE request	5	
OSCORE response	3	
Group OSCORE pairwise request	7	
Group OSCORE pairwise response	4	

Figure 7: Overhead (excluding ICV) in bytes (Connection/Sender ID = '', Sequence Number = '05')

Issues and planned content

- Update numbers based on draft-ietf-tls-ctls-08. The latest version updates a lot of the number in the examples.
  - Unclear if cTLS will support more efficient encoding for P-256 and ECDSA. E.g., the encodings in draft-mattsson-tls-compact-ecc. The latest version of cTLS changed the example from ECDSA to EdDSA.
  - P-256 and ECDSA are still the MTI algorithms in draft-ietf-uta-tls13-iot-profile-06
  - cTLS is still unstable.
- Verify overhead of draft-ietf-core-oscore-edhoc (might be 1-2 bytes wrong).
- Akran Sheriff wrote that EDHOC size is dependent on the key id. This is also true for cTLS.
  - Both EDHOC and cTLS depend on key id size. Very small relative difference…
  - Bigger impact would be splitting up DTLS flight #2 in several records as well as fragmentation.
  - Impact of tag length is simple and mentioned in text. CCM_8 is MTI in RFC 7925, EDHOC, and draft-ietf-uta-tls13-iot-profile
- Erik Kline pointed out correctly that the document should reference SCHC.
  - Should SCHC numbers be included? Anyone wants to measure overhead with SCHC?
- IOTOPS should decide high level on content. When that is done, we should publish.