Comparison of CoAP Security Protocols

draft-mattsson-lwig-security-protocol-comparison-01

John Mattsson, Ericsson
Francesca Palombini, Ericsson

IETF 101, lwig WG, London, Mar 21, 2018

Status Update

- Removed raza-6lo-compressed-dtls as suggested by Hannes Tschofenig
- Aligned to updated DTLS 1.3 (v-26)
  - Smaller header in DTLS 1.3
  - Added the DTLS 1.3 short header format
- Corrected legacy version number for TLS 1.3 (0x0303 instead of 0x0301)
- Added encrypted content type in TLS 1.3 and DTLS 1.3
- Removed the nonce from TLS 1.3
- Considerations about GHC: it increases the overhead for TLS 1.3 and DTLS 1.3

Status Update

- Added a table with overhead without MAC as suggested by Carsten Bormann
- Updated all the tables according to updates
- Updated summary according to updates

ToC

Summary

Updated numbers

Sequence Number	'05'	'1005'	'100005'
DTLS 1.2	29	29	29
DTLS 1.3	16	16	16
DTLS 1.3 (short header)	11	11	11
DTLS 1.2 (GHC)	16	16	16
DTLS 1.3 (GHC)	17	17	17
DTLS 1.3 (short header) (GCH)	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

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

Summary

New table

Protocol	Overhead	Overhead (GHC)
DTLS 1.2	21	8
DTLS 1.3	8	9
DTLS 1.3 (short header)	3	4
TLS 1.2	13	9
TLS 1.3	6	7
OSCORE Request	5	
OSCORE Response	3	

Figure 3: Overhead (excluding ICV) in bytes (Connection/Sender ID = '', Sequence Number = '05')

Next Steps

- Support at IETF100
- WG Adoption?