Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 3, 2018

J. Mattsson
Ericsson AB

September 30, 2017

Message Size Overhead of CoAP Security Protocols
draft-mattsson-core-security-overhead-01

Abstract

This document analyzes and compares 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, and OSCORE. DTLS and TLS are analyzed with and without compression. DTLS are analyzed with two different alternatives for header compression.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 3, 2018.

Table of Contents

1. Introduction

This document analyzes and compares per-packet message size overheads when using different security protocols to secure CoAP over UPD [RFC7252] and TCP [I-D.ietf-core-coap-tcp-tls]. The analyzed security protocols are DTLS 1.2 [RFC6347], DTLS 1.3 [I-D.rescorla-tls-dtls13], TLS 1.2 [RFC5246], TLS 1.3 [I-D.ietf-tls-tls13], and OSCORE [I-D.ietf-core-object-security]. The DTLS and TLS record layers are analyzed with and without compression. DTLS are analyzed with two different alternatives ([RFC7400] and [raza-6lo-compressed-dtls]) for header compression.

2. Overhead of Security Protocols

To enable comparison, all the overhead calculations in this section use AES-CCM with a tag length of 8 bytes, a plaintext of 6 bytes, and the sequence number '05'. This follows the example in [RFC7400], Figure 16.

2.1. DTLS 1.2

This example is taken directly from [RFC7400], Figure 16. The nonce follow the strict profiling given in [RFC7925].

DTLS 1.2 Record Layer (35 bytes, 29 bytes overhead):
17 fe fd 00 01 00 00 00 00 00 05 00 16 00 01 00
00 00 00 00 05 ae a0 15 56 67 92 4d ff 8a 24 e4
cb 35 b9

Content type:
17
Version:
fe fd
Epoch:
00 01
Sequence number:
00 00 00 00 00 05
Length:
00 16
Nonce:
00 01 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 gives 29 bytes overhead.

2.2. DTLS 1.2 with 6LoWPAN-GHC

Note that the compressed overhead is dependent on the parameters epoch, sequence number, and length. The following is only an example.

Note that the sequence number '01' used in [RFC7400], Figure 15 gives an exceptionally small overhead that is not representative.

Note that this header compression is not available when DTLS is exchanged over transports that do not use 6LoWPAN together with 6LoWPAN-GHC.

Compressed DTLS 1.2 Record Layer (22 bytes, 16 bytes overhead):
b0 c3 03 05 00 16 f2 0e ae a0 15 56 67 92 4d ff
8a 24 e4 cb 35 b9

Compressed DTLS 1.2 Record Layer Header and Nonce:
b0 c3 03 05 00 16 f2 0e
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

When compressed with 6LoWPAN-GHC, DTLS 1.2 with the above parameters (epoch, sequence number, length) gives 16 bytes overhead.

2.3. DTLS 1.2 with raza-6lo-compressed-dtls

Note that the compressed overhead is dependent on the parameters epoch and sequence number. The following is only an example.

Note that this header compression is not available when DTLS is exchanged over transports that do not use 6LoWPAN together with raza-6lo-compressed-dtls.

Compressed DTLS 1.2 Record Layer (19 bytes, 13 bytes overhead):
90 17 01 00 05 ae a0 15 56 67 92 4d ff 8a 24 e4
cb 35 b9

NHC
90
Compressed DTLS 1.2 Record Layer Header and Nonce:
17 01 00 05
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

When compressed with raza-6lo-compressed-dtls, DTLS 1.2 with the above parameters (epoch, sequence number) gives 13 bytes overhead.

2.4. DTLS 1.3

The only change compared to DTLS 1.2 is that the DTLS 1.3 record layer does not have an explicit nonce.

DTLS 1.3 Record Layer (27 bytes, 21 bytes overhead):
17 fe fd 00 01 00 00 00 00 00 05 00 0e ae a0 15
56 67 92 4d ff 8a 24 e4 cb 35 b9

Content type:
17
Version:
fe fd
Epoch:
00 01
Sequence number:
00 00 00 00 00 05
Length:
00 0e
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

DTLS 1.3 gives 21 bytes overhead.

2.5. DTLS 1.3 with 6LoWPAN-GHC

Note that the overhead is dependent on the parameters epoch, sequence number, and length. The following is only an example.

Note that this header compression is not available when DTLS is exchanged over transports that do not use 6LoWPAN together with 6LoWPAN-GHC.

Compressed DTLS 1.3 Record Layer (20 bytes, 14 bytes overhead):
b0 c3 11 05 00 0e ae a0 15 56 67 92 4d ff 8a 24
e4 cb 35 b9

Compressed DTLS 1.3 Record Layer Header and Nonce:
b0 c3 11 05 00 0e
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

When compressed with 6LoWPAN-GHC, DTLS 1.3 with the above parameters (epoch, sequence number, length) gives 14 bytes overhead.

2.6. DTLS 1.3 with raza-6lo-compressed-dtls

Note that the compressed overhead is dependent on the parameters epoch and sequence number. The following is only an example.

Note that this header compression is not available when DTLS is exchanged over transports that do not use 6LoWPAN together with raza-6lo-compressed-dtls.

Note that this header compression is not available when DTLS is exchanged over transports that do not use 6LoWPAN together with raza-6lo-compressed-dtls.

Compressed DTLS 1.3 Record Layer (19 bytes, 13 bytes overhead):
90 17 01 00 05 ae a0 15 56 67 92 4d ff 8a 24 e4
cb 35 b9

NHC
90
Compressed DTLS 1.3 Record Layer Header and Nonce:
17 01 00 05
c3 03 05 00 16 f2 0e
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

When compressed with raza-6lo-compressed-dtls, DTLS 1.3 with the above parameters (epoch, sequence number) gives 13 bytes overhead.

2.7. TLS 1.2

The changes compared to DTLS 1.2 is that the TLS 1.2 record layer does not have epoch and sequence number, and that the version is different.

TLS 1.2 Record Layer (27 bytes, 21 byte overhead):
17 03 03 00 16 00 00 00 00 00 00 00 05 ae a0 15
56 67 92 4d ff 8a 24 e4 cb 35 b9

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 gives 21 bytes overhead.

2.8. TLS 1.2 with 6LoWPAN-GHC

Note that the overhead is dependent on the parameters epoch, sequence number, and length. The following is only an example.

Note that this header compression is not available when TLS is exchanged over transports that do not use 6LoWPAN together with 6LoWPAN-GHC.

Compressed TLS 1.2 Record Layer (23 bytes, 17 bytes overhead):
05 17 03 03 00 16 85 0f 05 ae a0 15 56 67 92 4d
ff 8a 24 e4 cb 35 b9

Compressed TLS 1.2 Record Layer Header and Nonce:
05 17 03 03 00 16 85 0f 05
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

When compressed with 6LoWPAN-GHC, TLS 1.2 with the above parameters (epoch, sequence number, length) gives 17 bytes overhead.

2.9. TLS 1.3

The change compared to TLS 1.2 is that the TLS 1.3 record layer uses a different version.

TLS 1.3 Record Layer (27 bytes, 21 byte overhead):
17 03 01 00 16 00 00 00 00 00 00 00 05 ae a0 15
56 67 92 4d ff 8a 24 e4 cb 35 b9

Content type:
17
Version:
03 01
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 1.3 gives 21 bytes overhead.

2.10. TLS 1.3 with 6LoWPAN-GHC

Note that the overhead is dependent on the parameters epoch, sequence number, and length. The following is only an example.

Note that this header compression is not available when TLS is exchanged over transports that do not use 6LoWPAN together with 6LoWPAN-GHC.

Compressed TLS 1.3 Record Layer (23 bytes, 17 bytes overhead):
02 17 03 c3 01 16 85 0f 05 ae a0 15 56 67 92 4d
ff 8a 24 e4 cb 35 b9

Compressed TLS 1.3 Record Layer Header and Nonce:
02 17 03 c3 01 16 85 0f 05
Ciphertext:
ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

When compressed with 6LoWPAN-GHC, TLS 1.3 with the above parameters (epoch, sequence number, length) gives 17 bytes overhead.

2.11. OSCORE

Note that the overhead is dependent on the included CoAP Option numbers as well as the length of the OSCORE parameters Sender ID and sequence number.

Note that the sequence number '0' used in Example: Request 2 of [I-D.ietf-core-object-security], gives an exceptionally small overhead that is not representative.

The below calculation uses Option Delta = '9', and Sender ID = '0', and is only an example.

OSCORE Request (18 bytes, 12 bytes overhead):
91 0a 05 ec ae a0 15 56 67 92 4d ff 8a 24 e4
cb 35 b9

CoAP Option Delta and Length
91
Compressed COSE Header in Option Value:
0a
Compressed COSE Header in payload:
05
Ciphertext (including encrypted code):
ec ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

The below calculation uses Option Delta = '9', and Sender ID = '25', and is only an example.

OSCORE Request (19 bytes, 13 bytes overhead):
92 0a 25 05 ec ae a0 15 56 67 92 4d ff 8a 24 e4
cb 35 b9

CoAP Option Delta and Length
92
Compressed COSE Header in Option Value:
0a 25
Compressed COSE Header in payload:
05
Ciphertext (including encrypted code):
ec ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

The below calculation uses Option Delta = '9'

OSCORE Response (16 bytes, 10 bytes overhead):
90 ec ae a0 15 56 67 92 4d ff 8a 24 e4 cb 35 b9

CoAP Delta and Option Length:
90
Compressed COSE Header in Option Value:
-
Compressed COSE Header in payload:
-
Ciphertext (including encrypted code):
ec ae a0 15 56 67 92
ICV:
4d ff 8a 24 e4 cb 35 b9

OSCORE with the above parameters gives 13 bytes overhead for requests and 10 bytes overhead for responses. Clients having Sender ID = '0' gives an even smaller overhead (12 bytes) for requests.

Unlike DTLS and TLS, OSCORE has much smaller overhead for responses than requests.

3. OSCORE

4. Overhead with Different Sequence Numbers

The compression overhead (GHC) is dependent on the parameters epoch, sequence number, and length. The following overheads should be representative for sequence numbers with the same length.

The compression overhead (raza-6lo-compressed-dtls) is dependent on the length of the parameters epoch and sequence number. The following overheads apply for all sequence numbers with the same length.

The OSCORE overhead is dependent on the included CoAP Option numbers as well as the length of the OSCORE parameters Sender ID and sequence number.

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 (GHC)	16	16	17
DTLS 1.2 (Raza)	13	13	14
DTLS 1.3 (GHC)	14	14	15
DTLS 1.3 (Raza)	13	13	14
TLS 1.2 (GHC)	17	18	19
TLS 1.3 (GHC)	17	18	19
OSCORE Request (SID = 0)	12	13	14
OSCORE Request (SID = 1-255)	13	14	15
OSCORE Response	10	10	10

Figure 1: Overhead as a function of sequence number

5. Summary

DTLS 1.2 has quite a large overhead as it uses an explicit sequence number and an explicit nonce. DTLS 1.3, TLS 1.2, and TLS 1.3 have significantly less overhead.

Both DTLS compression methods provides very good compression. raza-6lo-compressed-dtls achieves slightly better compression but requires state. GHC is stateless but provides slightly worse compression. As DTLS 1.3 uses the same version number as DTLS 1.2, both GHC and raza-6lo-compressed-dtls works well also for DTLS 1.3.

The Generic Header Compression (6LoWPAN-GHC) is not that generic (the static dictionary is more or less a DTLS record layer) and the compression of TLS is not as good as the compression of DTLS. Similar compression levels as for DTLS could be achieved also for TLS, but this would require different static dictionaries for each version of TLS (as TLS 1.2 and TLS 1.3 uses different version numbers). GCH works very well as good for DTLS 1.3 as for DTLS 1.2 as the version number is the same.

The header compression is not available when (D)TLS is exchanged over transports that do not use 6LoWPAN together with 6LoWPAN-GHC or raza-6lo-compressed-dtls.

OSCORE has much lower overhead than DTLS and TLS. The overhead of OSCORE is smaller than DTLS over 6LoWPAN with compression, 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.

6. Security Considerations

This document is purely informational.

7. Acknowledgments

The authors want to thank Ari Keraenen for reviewing previous versions of the draft.

8. Informative References

[I-D.ietf-core-coap-tcp-tls]
Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., and B. Raymor, "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets", draft-ietf-core-coap-tcp-tls-09 (work in progress), May 2017.

[I-D.ietf-core-object-security]
Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", draft-ietf-core-object-security-05 (work in progress), September 2017.

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-21 (work in progress), July 2017.

[I-D.rescorla-tls-dtls13]
Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", draft-rescorla-tls-dtls13-01 (work in progress), March 2017.

[raza-6lo-compressed-dtls]
Raza, S., Shafagh, H., and O. Dupont, "Compression of Record and Handshake Headers for Constrained Environments", March 2017, <http://shahidraza.info/draft-raza-6lo-compressed.txt>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/info/rfc7400>.

[RFC7925] Tschofenig, H., Ed. and T. Fossati, "Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things", RFC 7925, DOI 10.17487/RFC7925, July 2016, <https://www.rfc-editor.org/info/rfc7925>.

Author's Address

John Mattsson
Ericsson AB
Faeroegatan 6
Kista SE-164 80 Stockholm
Sweden

Email: john.mattsson@ericsson.com