DTLS in SCTP

draft-westerlund-tsvwg-sctp-dtls-chunk-03
draft-westerlund-tsvwg-sctp-dtls-handshake-03

Magnus Westerlund
John Preuß Mattsson
Claudio Porfiri

IPR Declarations

- draft-westerlund-tsvwg-sctp-dtls-chunk-03
  - https://datatracker.ietf.org/ipr/6219/
- draft-westerlund-tsvwg-sctp-dtls-handshake-03
  - https://datatracker.ietf.org/ipr/6220/

Implementation Experience

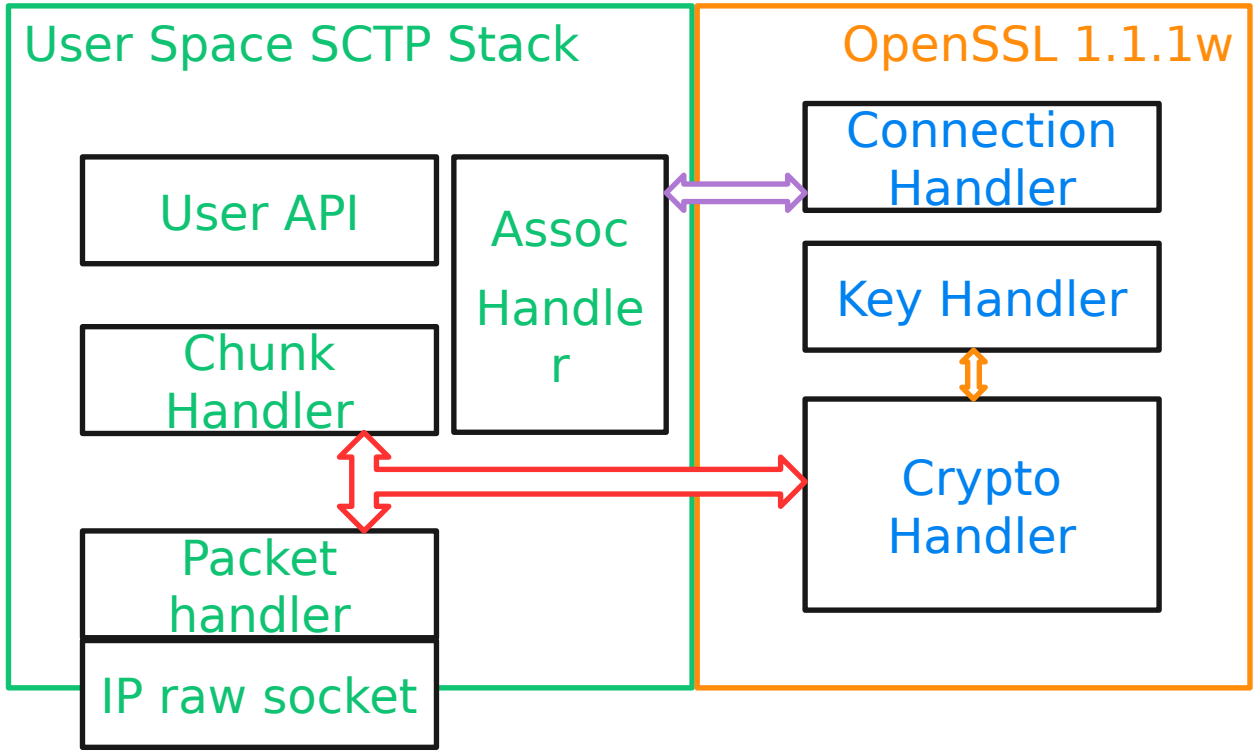
The PoC has been developed on User Space SCTP protocol stack owned by Ericsson and developed by Tieto.

Development activity was done by a team of 5 people and lasted 3 months, strictly using the drafts as input and adapting to OpenSSL 1.1.1 in Linux OS.

SCTP Client was also adapted as the API is slightly different, for instance it contains the rekeying interval parameters for the DTLS Connections.

The protocol stack has been verified on Linux clients, with the help of internal logging and Wireshark logs

The most common test cases have been executed, with focus on DTLS rekeying and Message segmentation/reassembly.



INITialization

1	12:47:38,602621	10.225.41.2	10.225.41.54	SCTP	88	INIT
2	12:47:38,606661	10.225.41.54	10.225.41.2	SCTP	276	INIT_ACK
3	12:47:38,607014	10.225.41.2	10.225.41.54	SCTP	248	COOKIE_ECHO
4	12:47:38,630666	10.225.41.54	10.225.41.2	SCTP	56	COOKIE_ACK
5	12:47:38,651105	10.225.41.2	10.225.41.54	SCTP	304	DATA (TSN=23302188)
6	12:47:38,656662	10.225.41.54	10.225.41.2	SCTP	56	COOKIE_ACK
7	12:47:38,656671	10.225.41.54	10.225.41.2	SCTP	152	DATA (TSN=15979772)
8	12:47:38,657089	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979772, Arwnd=16384)
9	12:47:38,658660	10.225.41.54	10.225.41.2	SCTP	56	COOKIE_ACK
10	12:47:38,658667	10.225.41.54	10.225.41.2	SCTP	1520	DATA (TSN=15979773) (Message Fragment)
11	12:47:38,658673	10.225.41.54	10.225.41.2	SCTP	56	COOKIE_ACK
12	12:47:38,658676	10.225.41.54	10.225.41.2	SCTP	280	DATA (TSN=15979774)
13	12:47:38,658684	10.225.41.54	10.225.41.2	SCTP	56	COOKIE_ACK
14	12:47:38,658687	10.225.41.54	10.225.41.2	SCTP	392	DATA (TSN=15979775)
15	12:47:38,658691	10.225.41.54	10.225.41.2	SCTP	56	COOKIE_ACK
16	12:47:38,658694	10.225.41.54	10.225.41.2	SCTP	148	DATA (TSN=15979776)
17	12:47:38,658697	10.225.41.54	10.225.41.2	SCTP	56	COOKIE_ACK
18	12:47:38,658700	10.225.41.54	10.225.41.2	SCTP	96	DATA (TSN=15979777)
19	12:47:38,658703	10.225.41.54	10.225.41.2	SCTP	68	SACK (Ack=23302188, Arwnd=16384)
20	12:47:38,658994	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979773, Arwnd=14932)
21	12:47:38,662881	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979774, Arwnd=16384)
22	12:47:38,663460	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979775, Arwnd=16384)
23	12:47:38,663845	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979776, Arwnd=16384)
24	12:47:38,667820	10.225.41.2	10.225.41.54	SCTP	1520	DATA (TSN=23302189) (Message Fragment)
25	12:47:38,667885	10.225.41.2	10.225.41.54	SCTP	280	DATA (TSN=23302190)
26	12:47:38,667995	10.225.41.2	10.225.41.54	SCTP	128	DATA (TSN=23302191)
27	12:47:38,668153	10.225.41.2	10.225.41.54	SCTP	356	DATA (TSN=23302192)
28	12:47:38,668272	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979777, Arwnd=16384)
29	12:47:38,670662	10.225.41.54	10.225.41.2	SCTP	68	SACK (Ack=23302189, Arwnd=14932)
30	12:47:38,672661	10.225.41.54	10.225.41.2	SCTP	68	SACK (Ack=23302190, Arwnd=16384)
31	12:47:38,674660	10.225.41.54	10.225.41.2	SCTP	68	SACK (Ack=23302191, Arwnd=16384)
32	12:47:38,674665	10.225.41.54	10.225.41.2	SCTP	68	SACK (Ack=23302192, Arwnd=16384)
33	12:47:38,675059	10.225.41.2	10.225.41.54	SCTP	84	DATA (TSN=23302193)
34	12:47:38,678660	10.225.41.54	10.225.41.2	SCTP	68	SACK (Ack=23302193, Arwnd=16384)
35	12:47:38,678888	10.225.41.2	10.225.41.54	SCTP	132	DATA (TSN=23302194)
36	12:47:38,682659	10.225.41.54	10.225.41.2	SCTP	84	DATA (TSN=15979778)
37	12:47:38,682665	10.225.41.54	10.225.41.2	SCTP	68	SACK (Ack=23302194, Arwnd=16384)
38	12:47:38,682910	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979778, Arwnd=16384)
39	12:47:38,686666	10.225.41.54	10.225.41.2	SCTP	132	DATA (TSN=15979779)
40	12:47:38,687216	10.225.41.2	10.225.41.54	SCTP	104	RESERVED
41	12:47:38,687355	10.225.41.2	10.225.41.54	SCTP	68	SACK (Ack=15979779, Arwnd=16384)
42	12:47:38,690661	10.225.41.54	10.225.41.2	SCTP	104	RESERVED
43	12:47:42,632673	10.225.41.54	10.225.41.2	SCTP	176	RESERVED
44	12:47:42,633092	10.225.41.2	10.225.41.54	SCTP	176	RESERVED
45	12:47:42,650317	10.225.41.2	10.225.41.54	SCTP	176	RESERVED

DTLS Connection Handshake

INIT

```
Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
Linux cooked capture v2
Internet Protocol Version 4, Src: 10.225.41.2, Dst: 10.225.41.54
Stream Control Transmission Protocol, Src Port: 1001 (1001), Dst Port: 2001 (2001)
    Source port: 1001
    Destination port: 2001
    Verification tag: 0x00000000
    [Association index: disabled (enable in preferences)]
    Checksum (CRC32C): 0xdc166f97 [correct]
    [Checksum Status: Good]
  INIT chunk (Outbound streams: 2, inbound streams: 2)
    Chunk type: INIT (1)
        0... .... = Bit: Stop processing of the packet
        .0.. .... = Bit: Do not report
      Chunk flags: 0x00
      Chunk length: 36
      Initiate tag: 0x0163902c
      Advertised receiver window credit (a_rwnd): 16384
      Number of outbound streams: 2
      Number of inbound streams: 2
      Initial TSN: 23302188
    Cookie preservative parameter (Increment :0 msec)
    Unknown parameter (Type 32773, value length: 4 bytes)
      Parameter type: Unknown (0x8005)
      Parameter length: 8
      Parameter value: 00010002
```

```
0000  08 00 00 00 00 00 00 5e  00 01 04 06 7c 72 6e 97   .......^ ....|rn.
0010  41 73 00 00 45 a0 00 44  12 cd 00 00 40 84 fe cf   As..E..D ....@...
0020  0a e1 29 02 0a e1 29 36  03 e9 07 d1 00 00 00 00   ..)...)6 ........
0030  dc 16 6f 97 01 00 00 24  01 63 90 2c 00 00 40 00   ..o....$ .c.,..@.
0040  00 02 00 02 01 63 90 2c  00 09 00 08 00 00 00 00   .....c., ........
0050  80 05 00 08 00 01 00 02                           ........
```

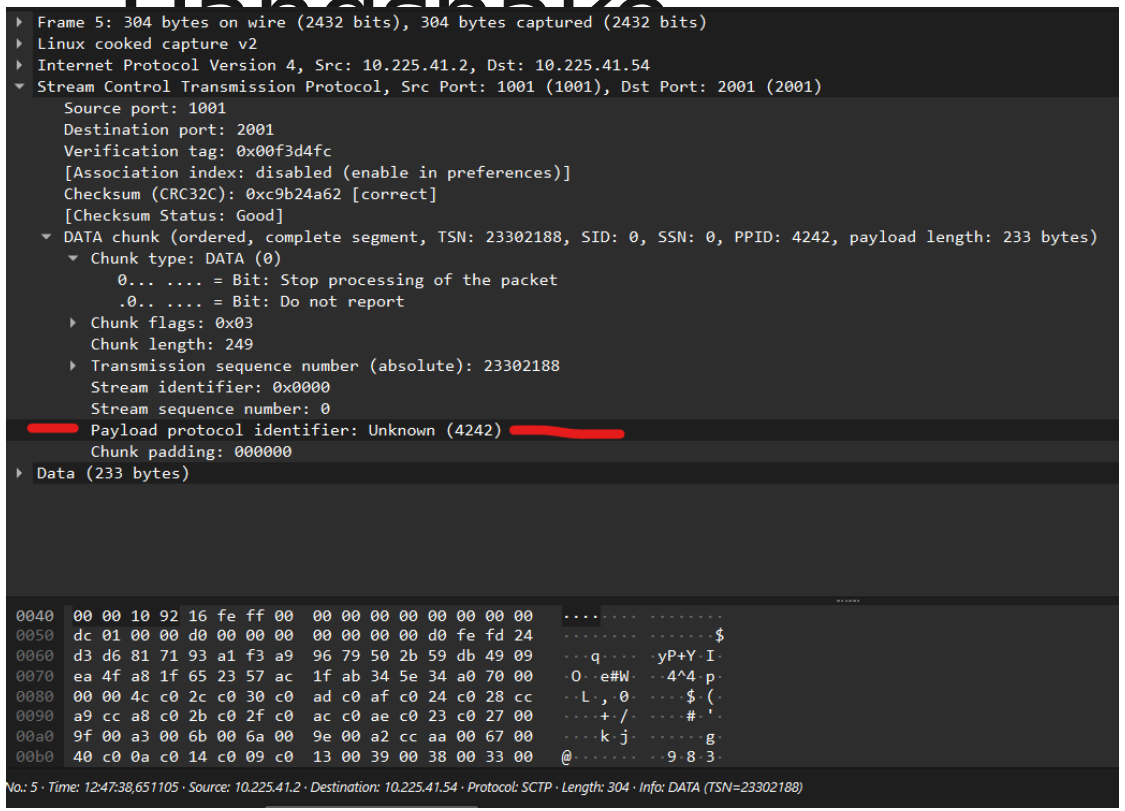
INIT ACK

```
Frame 2: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits)
Linux cooked capture v2
Internet Protocol Version 4, Src: 10.225.41.54, Dst: 10.225.41.2
Stream Control Transmission Protocol, Src Port: 2001 (2001), Dst Port: 1001 (1001)
    Source port: 2001
    Destination port: 1001
    Verification tag: 0x0163902c
    [Association index: disabled (enable in preferences)]
    Checksum (CRC32C): 0xa0c7e77c [correct]
    [Checksum Status: Good]
  INIT_ACK chunk (Outbound streams: 2, inbound streams: 2)
    Chunk type: INIT_ACK (2)
        0... .... = Bit: Stop processing of the packet
        .0.. .... = Bit: Do not report
      Chunk flags: 0x00
      Chunk length: 224
      Initiate tag: 0x00f3d4fc
      Advertised receiver window credit (a_rwnd): 16384
      Number of outbound streams: 2
      Number of inbound streams: 2
      Initial TSN: 15979772
    Unknown parameter (Type 32773, value length: 4 bytes)
      Parameter type: Unknown (0x8005)
      Parameter length: 8
      Parameter value: 00010002
    State cookie parameter (Cookie length: 192 bytes)
```

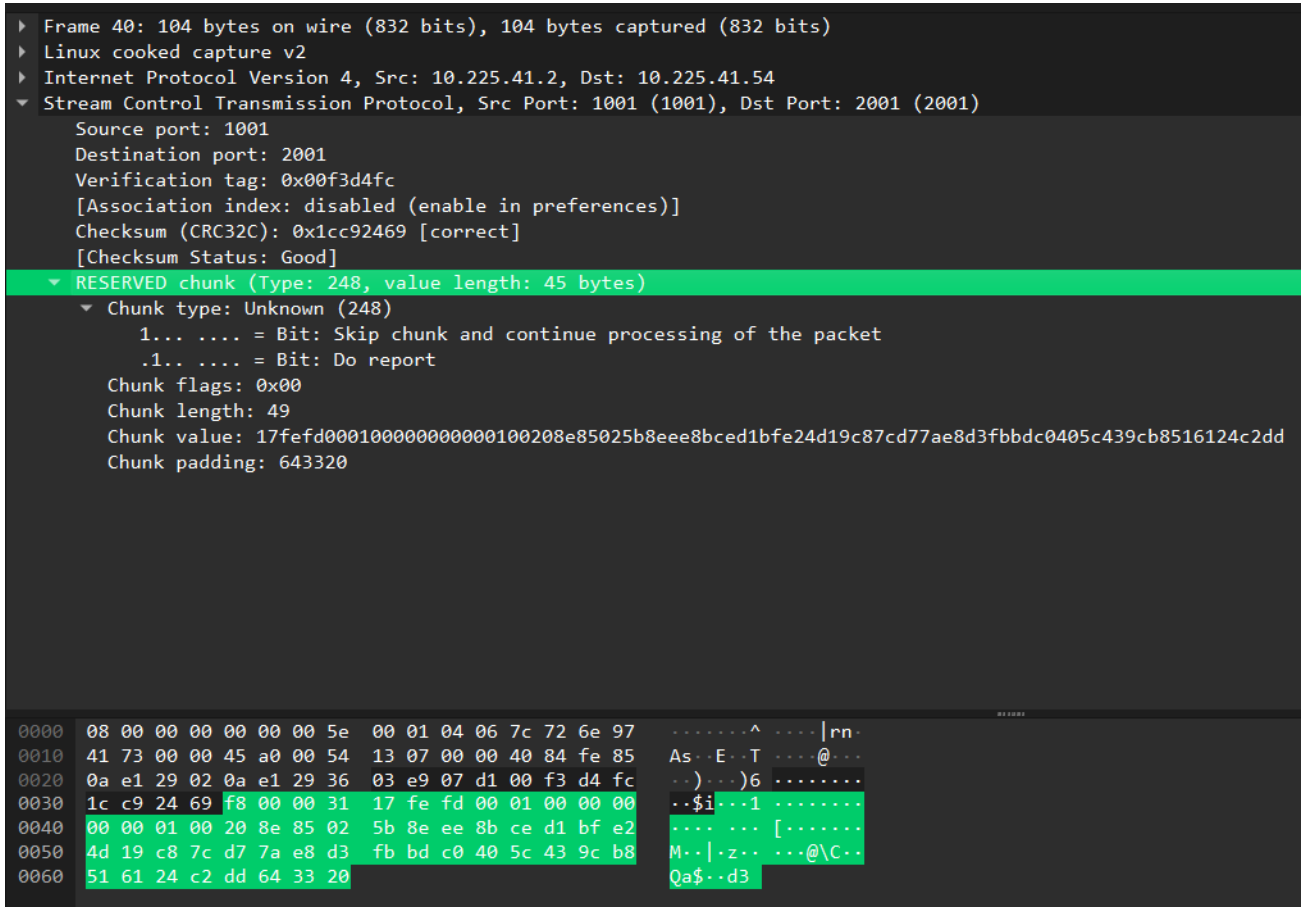
```
0040  00 02 00 02 00 f3 d4 fc  80 05 00 08 00 01 00 02   ........ ........
0050  00 07 00 c4 03 e9 07 d1  00 f3 d4 fc 01 63 90 2c   ........ .....c.,
0060  00 f3 d4 fc 01 63 90 2c  00 00 00 00 00 00 00 00   .....c., ........
0070  00 00 40 00 00 00 40 00  00 02 00 02 00 00 1a fc   ..@...@. ........
0080  00 00 00 c5 00 00 1a c0  00 00 00 c5 00 00 00 01   ........ ........
0090  00 00 00 01 00 00 00 00  00 00 00 00 0a e1 29 02   ........ ......).
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 0a e1 29 36  00 00 00 00 00 00 00 00   ......)6 ........
```

No.: 2 · Time: 12:47:38,606661 · Source: 10.225.41.54 · Destination: 10.225.41.2 · Protocol: SCTP · Length: 276 · Info: INIT_ACK

DTLS Handshake



Data Transfer



REKEY by means of new DTLS Connection

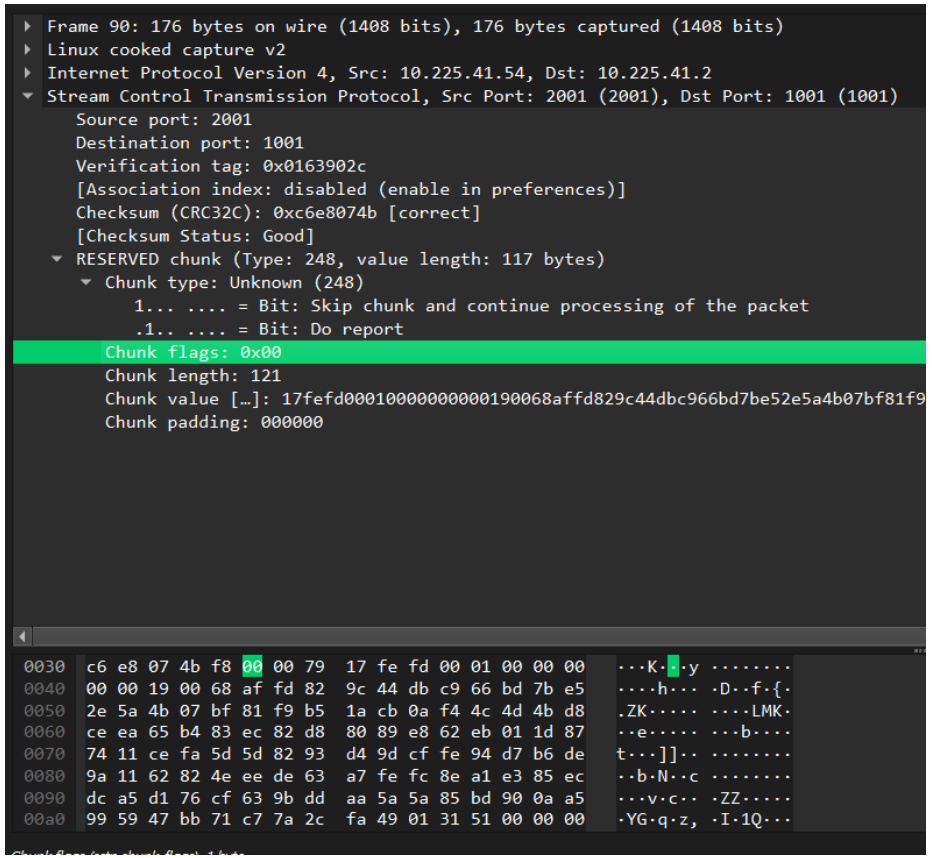
CID = 0

CID = 1

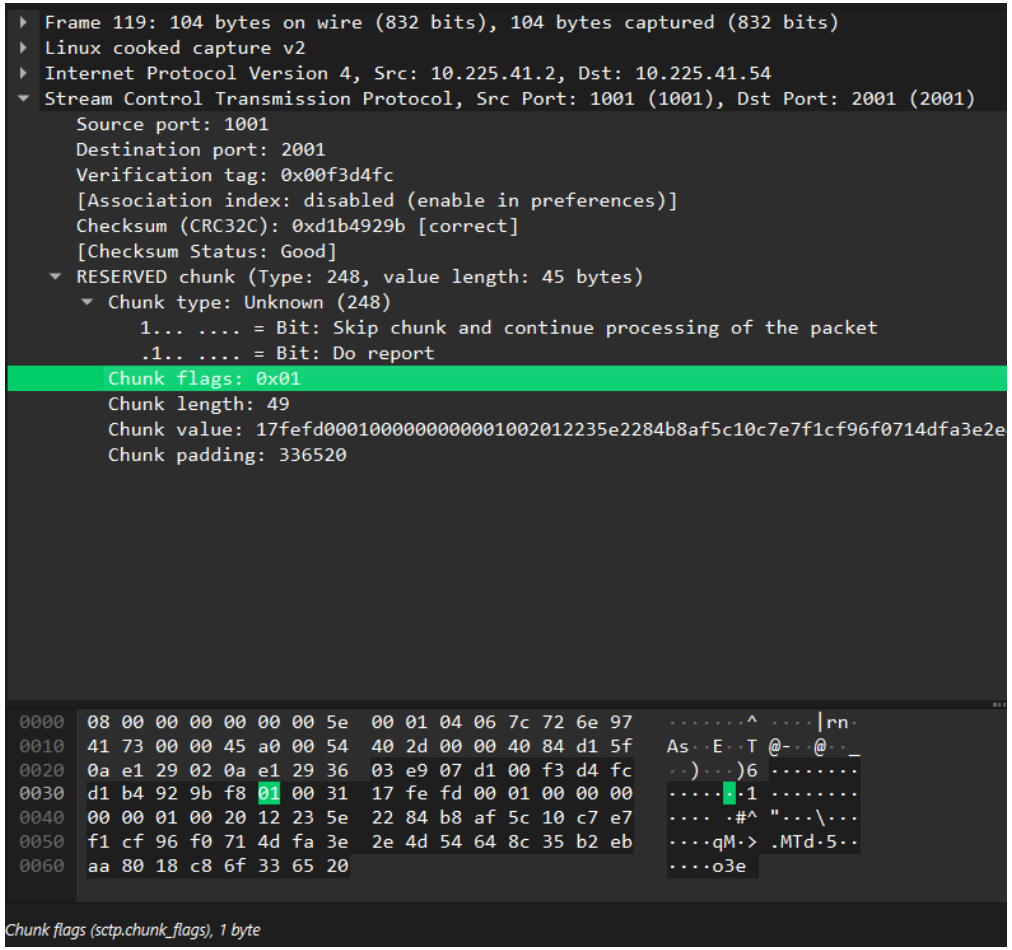
87	12:48:06,836671	10.225.41.54	10.225.41.2	SCTP	176 RESERVED
88	12:48:06,837126	10.225.41.2	10.225.41.54	SCTP	176 RESERVED
89	12:48:06,850369	10.225.41.2	10.225.41.54	SCTP	176 RESERVED
90	12:48:06,852660	10.225.41.54	10.225.41.2	SCTP	176 RESERVED
91	12:48:08,687771	10.225.41.2	10.225.41.54	SCTP	304 DATA (TSN=23302195)
92	12:48:08,692663	10.225.41.54	10.225.41.2	SCTP	152 DATA (TSN=15979780)
93	12:48:08,692673	10.225.41.54	10.225.41.2	SCTP	1416 DATA (TSN=15979781) (Message Fragment)
94	12:48:08,692679	10.225.41.54	10.225.41.2	SCTP	384 DATA (TSN=15979782)
95	12:48:08,692683	10.225.41.54	10.225.41.2	SCTP	392 DATA (TSN=15979783)
96	12:48:08,692687	10.225.41.54	10.225.41.2	SCTP	148 DATA (TSN=15979784)
97	12:48:08,692691	10.225.41.54	10.225.41.2	SCTP	96 DATA (TSN=15979785)
98	12:48:08,693263	10.225.41.2	10.225.41.54	SCTP	112 RESERVED
99	12:48:08,694663	10.225.41.54	10.225.41.2	SCTP	112 RESERVED
100	12:48:08,697717	10.225.41.2	10.225.41.54	SCTP	112 RESERVED
101	12:48:08,698215	10.225.41.2	10.225.41.54	SCTP	112 RESERVED
102	12:48:08,698564	10.225.41.2	10.225.41.54	SCTP	112 RESERVED
103	12:48:08,701632	10.225.41.2	10.225.41.54	SCTP	1416 DATA (TSN=23302196) (Message Fragment)
104	12:48:08,701703	10.225.41.2	10.225.41.54	SCTP	384 DATA (TSN=23302197)
105	12:48:08,701811	10.225.41.2	10.225.41.54	SCTP	128 DATA (TSN=23302198)
106	12:48:08,701987	10.225.41.2	10.225.41.54	SCTP	356 DATA (TSN=23302199)
107	12:48:08,702123	10.225.41.2	10.225.41.54	SCTP	112 RESERVED
108	12:48:08,704666	10.225.41.54	10.225.41.2	SCTP	112 RESERVED
109	12:48:08,708664	10.225.41.54	10.225.41.2	SCTP	112 RESERVED
110	12:48:08,708675	10.225.41.54	10.225.41.2	SCTP	112 RESERVED
111	12:48:08,708679	10.225.41.54	10.225.41.2	SCTP	112 RESERVED
112	12:48:08,709362	10.225.41.2	10.225.41.54	SCTP	84 DATA (TSN=23302200)
113	12:48:08,712660	10.225.41.54	10.225.41.2	SCTP	112 RESERVED
114	12:48:08,712946	10.225.41.2	10.225.41.54	SCTP	132 DATA (TSN=23302201)
115	12:48:08,716661	10.225.41.54	10.225.41.2	SCTP	84 DATA (TSN=15979786)
116	12:48:08,716668	10.225.41.54	10.225.41.2	SCTP	112 RESERVED
117	12:48:08,716969	10.225.41.2	10.225.41.54	SCTP	112 RESERVED
118	12:48:08,720661	10.225.41.54	10.225.41.2	SCTP	132 DATA (TSN=15979787)
119	12:48:08,721156	10.225.41.2	10.225.41.54	SCTP	104 RESERVED
120	12:48:08,721317	10.225.41.2	10.225.41.54	SCTP	112 RESERVED
121	12:48:08,724661	10.225.41.54	10.225.41.2	SCTP	104 RESERVED

New DTLS Connection Handshake

Data transfer with different CID



CID = 0



CID = 1

Lessons learned

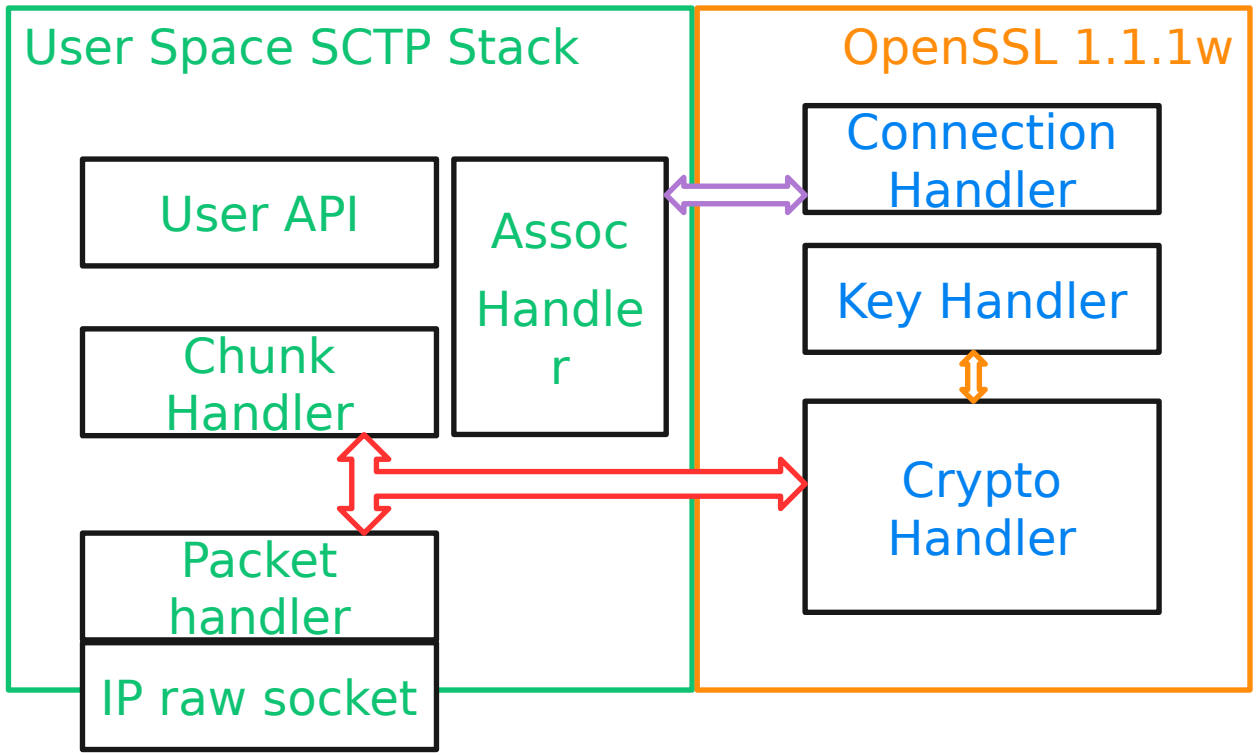
The PoC demo is based on DTLS 1.2 because the OpenSSL library used does not yet support DTLS 1.3.

Different messages sizes have been tested, with MTU length from 100 bytes up to 8 kbytes

As expected, rekeying is smooth and doesn’t affect traffic latency

With small packets, for instance “paging” (~100 bytes) and message bundling, DTLS in SCTP encryption use is very efficient.

Having a Wireshark SCTP parser that supported this draft would have simplified debugging.



Lessons learned

PVALID retransmissions

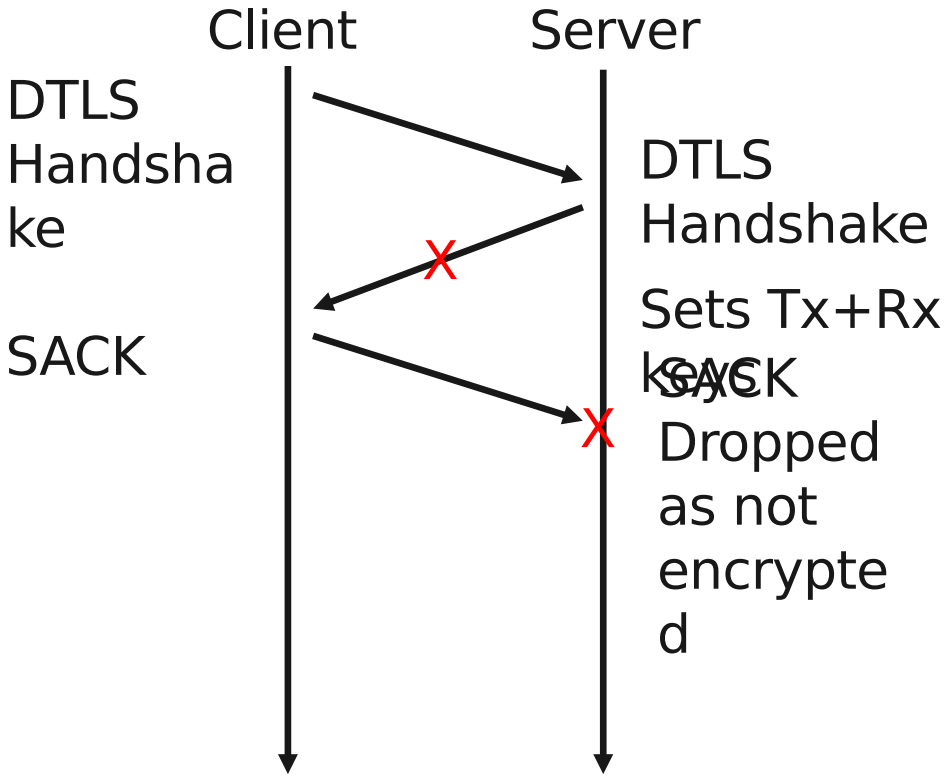
- Found a race conditions that could deadlock entering Validation
- Clarified the need to first install receive keys then enable sending encrypted chunk when sending PVALID

Security Solutions Options with Chunk Protected

- Stack supports RFC 6083
- Multiple set of parameters requires evaluating all parameters and select the most appropriate

DTLS Handshake for rekeying uses plain DATA with PPID=4242

- This exposes endpoint to security weaknesses where attacker manipulates receiver window using DATA chunks with PPID=4242
- Spec now requires encryption of all chunks including rekeying DTLS Handshake after endpoint has reached PROTECTED state



Further Updates

- Chunks
  - Optimization for completing VALIDATION if the PVALID response packet was lost and encrypted data would appear
  - Privacy consideration has been clarified
  - AEAD Limits clarification
- Handshake
  - Clarified on removal of DTLS sessions