DTLS for SCTP

https://datatracker.ietf.org/doc/draft-ietf-tsvwg-dtls-over-sctp-bis/

https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-crypto-chunk/
https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-crypto-dtls/

Magnus Westerlund
John Preuß Mattsson
Claudio Porfiri

Goal of this presentation

- Enable the WG to:
  - Consider the requirements on a solution
  - Present the different trade-off between the proposals
  - A future consensus call on a direction for the DTLS security solution

- This presentation is focused on what is needed to meet 3GPP Request
  - No change to earlier agreement to not deprecate RFC 6083
  - draft-tuexen-tsvwg-rfc6083-bis to address update to DTLS 1.3 and Security Issues without additional changes are proposed

IPR Declarations

- draft-ietf-tsvwg-dtls-over-sctp-bis
  - https://datatracker.ietf.org/ipr/5195/
  - https://datatracker.ietf.org/ipr/5218/
- draft-westerlund-tsvwg-sctp-crypto-chunk
  - None
- draft-westerlund-tsvwg-sctp-crypto-dtls
  - https://datatracker.ietf.org/ipr/5969/
  - https://datatracker.ietf.org/ipr/5968/

Background

- https://datatracker.ietf.org/liaison/1723/ (Received 2021-03-05) from 3GPP RAN3

1. Overall Description:

From the first version of the 5G specification, 3GPP has specified to use DTLS over SCTP. RAN3 has found an issue related to RFC 6083 DTLS user message size limitation over SCTP that impacts several of 3GPP RAN application protocols. The RFC specifies a user message limit of approximate16k Bytes. This should be compared to the unlimited user message size that exists when SCTP is used without DTLS.

There are several RAN application messages that can exceed the limit of approximate 16k Bytes. The same issue may exist for the other 3GPP groups using the DTLS over SCTP.

A general solution to this issue is desirable rather than changing multiple different protocols. We understand the limitation in RFC 6083 is due to a lack of a secure fragmentation mechanism of user messages into multiple DTLS records. The DTLS over SCTP specification appear to be the right layer to resolve this issue and achieve feature parity between DTLS over SCTP and unsecured SCTP.

RAN3 would like to ask the IETF TSVWG to investigate and would greatly appreciate a solution to the issue related to the size limitation for DTLS over SCTP. 2.

Actions:

To IETF TSVWG group. ACTION: RAN3 kindly asks IETF TSVWG to investigate the possibility to remove the size limitation issue in DTLS over SCTP and provide feedback to RAN3.

Background

- Liaison statement from 3GPP SA3 received on 2023-06-07: https://datatracker.ietf.org/liaison/1847/

1 Overall description

SA3 would like to thank IETF Transport Area Working Group (TSVWG) for notifying SA3 of the vulnerabilities related to SCTP-AUTH and DTLS over SCTP.

SA3 agrees that the vulnerabilities are serious – they are affecting confidentiality, integrity, replay, and availability. Supporting DTLS over SCTP in N2, Xn, F1, and E1 interfaces has been made mandatory from Release 15 onwards. Therefore, SA3's understanding is that it is important to solve all the security vulnerabilities, including the availability vulnerabilities. Since the problem is related to the use of DTLS with SCTP, SA3's understanding is that the solution should be based on DTLS, and the solution should not rely on unsupported DTLS features

SA3 kindly asks TSVWG to work on and publish a solution as soon as possible.

2 Actions

To: IETF Transport Area Working Group (TSVWG)

ACTION: SA3 kindly asks IETF Transport Area Working Group (TSVWG) to take the above information into account and keep SA3 updated on TSVWG's.

3 Dates of next TSG SA WG 3 meetings

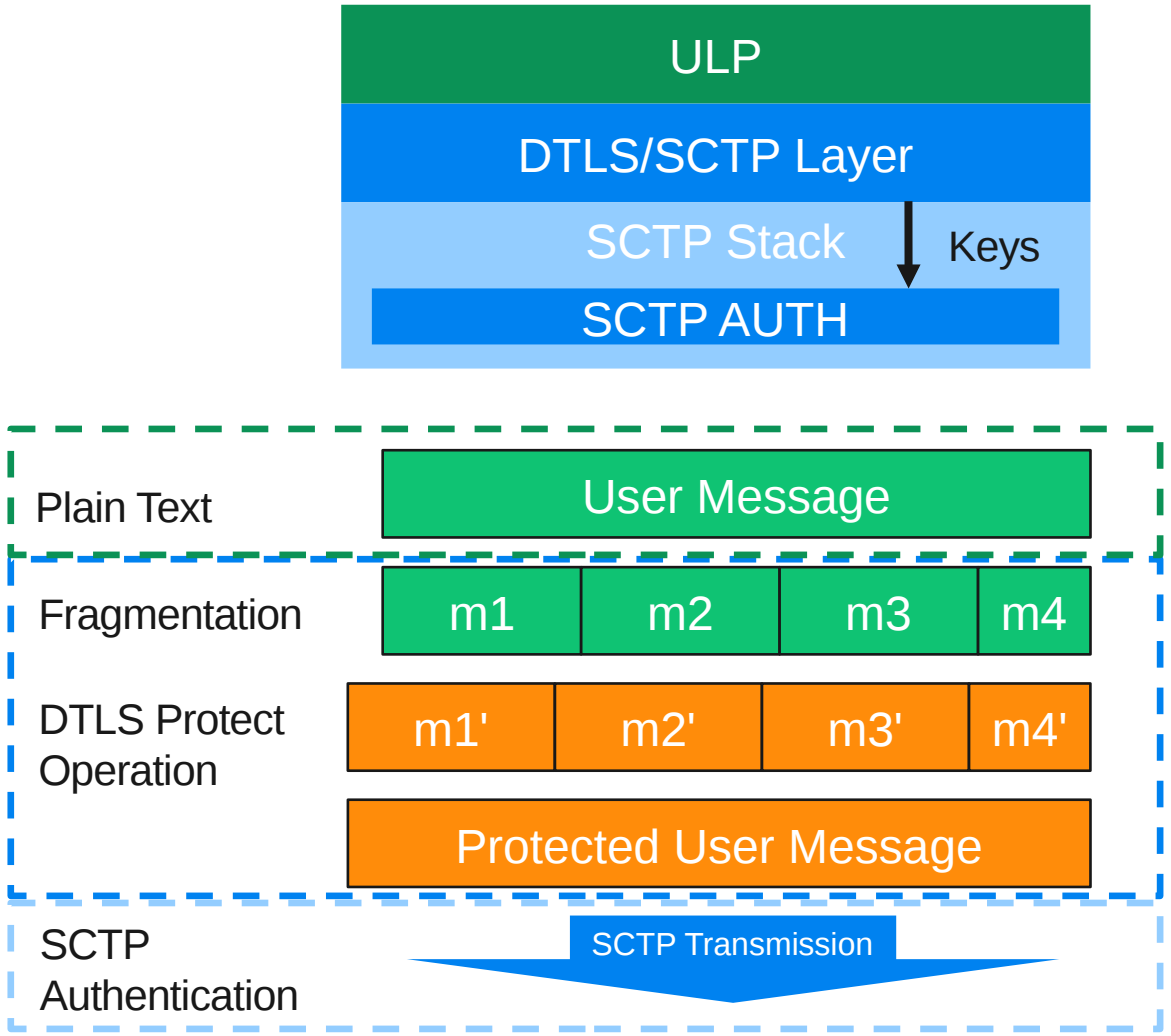
SA3#112	14 - 18 August 2023	Goteborg, Sweden
SA3#113	6 - 10 November 2023	Chicago, USA

Requirements

- 3GPP Requirements as interpreted by authors:
  - Support the 3GPP Application protocols potential message sizes:
    - S1-AP (3GPP TS 36.413): 142 kbyte
    - Xn (3GPP TS 48.423): > 500 kbyte
  - Support the protocols potential very long life-time expectation of many weeks for the SCTP association
  - Acknowledge that terminating the SCTP association can have significant impact on the mobile network:
    - Negatively impacting SCTP association availability not acceptable
  - Mutual re-authentication
    - For the 3GPP control signaling it is important to be able to know the identity of the peer and verify it
- Good modern security practices:
  - Forward secrecy
  - Periodic rekeying with (EC)DHE to force dynamic key exfiltration

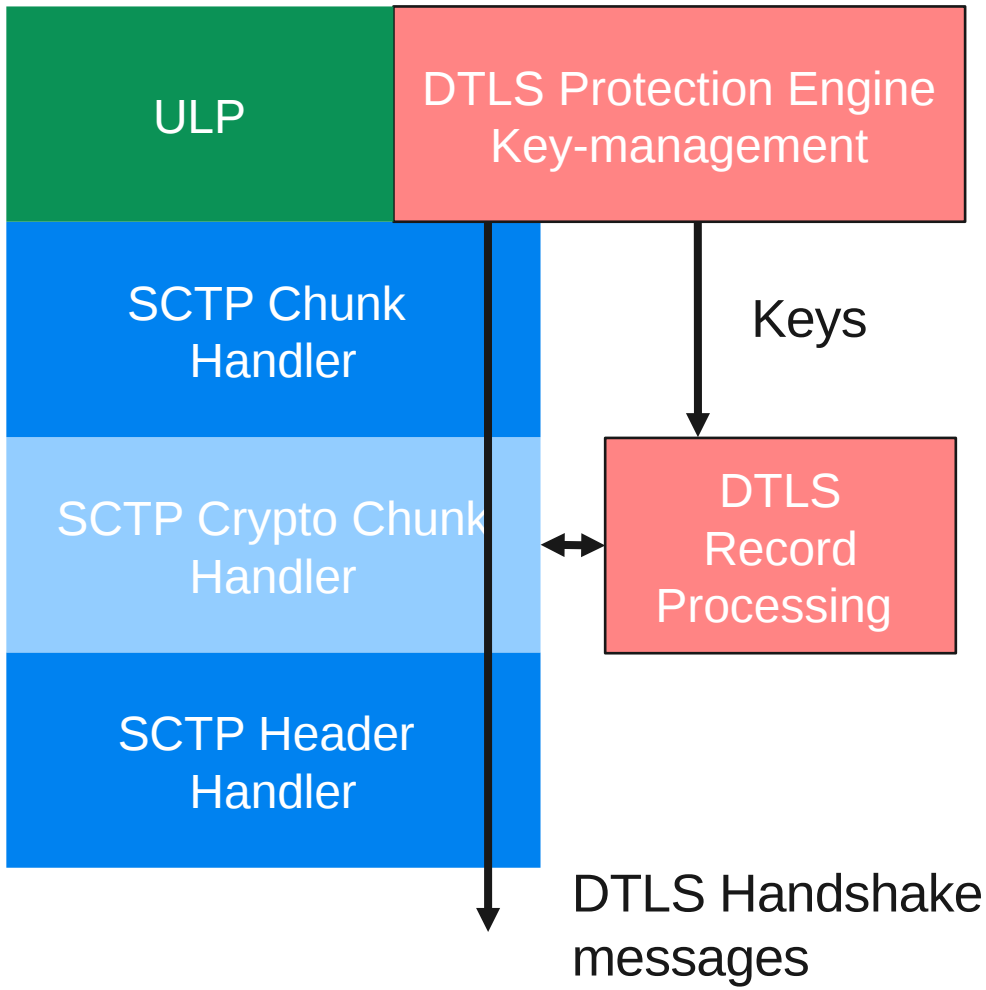
The Proposals: DTLS over SCTP

- DTLS over SCTP (SCTP/DTLS)
  - https://datatracker.ietf.org/doc/draft-ietf-tsvwg-dtls-over-sctp-bis/
  - https://datatracker.ietf.org/doc/draft-tuexen-tsvwg-rfc4895-bis/
- An Adaptation layer between Upper Layer Protocol (ULP)
  - Fragments user messages into multiple fragments
  - Each fragment protected by a DTLS record
- Relies on SCTP-AUTH to ensure record order
  - DTLS keys the SCTP-AUTH
- Uses parallel DTLS connection for rekeying
  - Use DTLS Connection IDs for identification



The Proposals: DTLS in Crypto Chunk

- DTLS in SCTP (DTLS in Crypto Chunks)
  - https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-crypto-dtls/
  - https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-crypto-chunk/
- Crypto Chunk is a new SCTP Chunk
  - Encapsulated all other chunks in a crypto envelope on per SCTP packet basis
- DTLS is a protection engine
  - DTLS handshake messages sent as SCTP messages in DATA chunks using a specific PPID
  - After DTLS keys are established all future SCTP packet's contents are protected
  - At rekeying perform handshake for a new DTLS connection
- Fragmentation done by SCTP's normal message fragmentation mechanism



DTLS Implementation requirements

	DTLS in Crypto Chunk	SCTP/DTLS
DTLS Versions	1.2 and 1.3	1.2 and 1.3
DTLS Connection ID required	No	Yes
Replay protection	May be used	Must be turned off
Key-Update	May be used	Must be turned off
DTLS Record Sizes	SCTP Packet MTU	16384 bytes or require RFC 8449
Stack availability	1.2: Yes, OpenSSL and many other 1.3: WolfSSL	1.2: MbedTLS? 1.3: Unknown

Rekeying Robustness

DTLS in SCTP Chunks:

- When necessary to rekey, periodic or data limits initiate a new DTLS handshake as SCTP messages with PPID
- When keys have been derived install them for reception related to Crypto Chunk flag field DCID
- When handshakes completes start using new keys
- Leave old keys in place to drain network of SCTP packets protected by old key
  - A MSL (2 min) timer is sufficient
  - Close old DTLS connection
- As soon as both sides have keys, i.e. after handshake acks one can switch
  - Will at worst induce some packet loss

SCTP/DTLS:

- When necessary to rekey, initiate a new DTLS connection. Using DTLS connection IDs to separate the old and new DTLS Connection
  - Export key from DTLS connection to SCTP-AUTH
- Start using new DTLS connection for records and in SCTP-AUTH
  - RFC 6458 API if only enables setting SCTP-AUTH key on new SCTP messages
- DTLS Connection can’t be closed until:
  - All DTLS records protected by that session have been decrypted
    - Data loss if not done correctly -> Need to abort SCTP Association
  - RFC 6458 API requires draining whole session to know when all has been delivered
  - To avoid draining, implementation needs to
    - track what DTLS session was used on which DTLS records
    - know which data offsets they represent in messages
    - And know when they been non-renegable ACKed

SCTP Replay Protection

DTLS in Crypto Chunk

- DTLS replay protection can be utilized to ensure replay of older SCTP packets would not be possible.
- That would ensure that old SCTP packets with control chunks would not be able to impact the SCTP association
- Replay window needs to be scaled based on expected re-ordering between paths
- Strong protection against availability attacks

SCTP/DTLS

- Assumes that SCTP-AUTH directionality issue is fixed
- Data replay can occur after TSN wrap (2^32 Data Chunks)
  - SACK replay can declare non received DATA after TSN wrap ACKed and lock up SCTP association
  - Mitigation is to rekey and retire SCTP-AUTH keys more frequently than TSN wraps
- SCTP have no general protection against replay attacks
  - Risks for most chunks appear to be low
  - Error chunk replay might trigger strange behavior and would be implementation dependent
- Each rekeying would minimize the window from where packet can be replayed
  - Lack of encryption simplifies targeted replay choosing the packets with potential impact

Performance and Trust

DTLS in Crypto Chunk

- Performs a single set of cipher operations on each record
  - Depending on cipher
- General trust in DTLS is good as living and maintained protocol
- Contains new things to implement and analyze

SCTP/DTLS

- Performs
  - First DTLS cipher operation on content of DATA chunks
  - SCTP-AUTH protection of SCTP packet content using HMAC-SHA256
- General trust in DTLS
- Trust in SCTP-AUTH is much less
  - Few implementation
  - No academic review of properties
  - Found issues being addressed
- Contains new things to implement and analyze

Message size limits

DTLS in Crypto Chunk:

- No limitation exist as per normal SCTP

SCTP/DTLS

- With good SCTP APIs and tracking
  - No Limit exists
- Using RFC 6458 API
  - Message must not take longer time to transfer than time between rekeyings
  - The limitation in setting SCTP-AUTH key to use when sending causes this limit
    - Can’t rekey again until the message has concluded and the old DTLS connection is retired

No expected impact on known 3GPP application usage

Implementation Impact

DTLS in Crypto Chunk:

- Requires implementing the Crypto Chunk in SCTP stack
  - Potential kernel impact
- DTLS protection engine wrapping of DTLS
- Expect to available DTLS implementations to work
- Kernel implementation of DTLS record protection
  - Split DTLS implementation
  - New API for crypto context

SCTP/DTLS:

- Update of SCTP-AUTH required in SCTP Stack
  - Potential kernel impact
- SCTP tracking of delivered data update in SCTP stack plus API
- DTLS implementation likely requires update to support necessary features
  - DTLS connection ID
- SCTP/DTLS logic as adaptation layer (user land)

Summary of differences

	DTLS in Crypto Chunk	SCTP/DTLS
DTLS Implementation availability	Reasonable	Poor
Rekeying Robustness	Good	Poor
Message Size	Unlimited	Large but impacting rekeying
Encrypting SCTP control chunks	Yes	No, only authentication
Replay Protecting SCTP Control chunks	Yes	None, dependent on SCTP robustness and rekeying
Crypto Passes on Data	DTLS only	First DTLS, then SCTP-AUTH
Implementation impact	Medium to high (Kernel)	Medium to high (DTLS implementation)

Which way forward do we choose?

- Want to get the solution choice done
  - Lack of solution prevents vendors to implement and operators to deploy this security
  - Expect upwards a year from direction chosen to finalize the spec
- Proposed way forward
  - Schedule an Interim meeting on this topic in September
  - Target a consensus call after the Interim meeting
  - Send Liaison statement to 3GPP SA3 and RAN3 to;
    - Inform them about the interim meeting and invite to participate
    - Request any clarification on requirements and additional input that can affect the choice