DTLS based Security for SCTP
Report from Design Team

2024-02-23
Design Team Participants

- Marcelo Ricardo Leitner
- Xin Long
- John Mattsson
- Claudio Porfiri
- Tirumaleswar Reddy.K
- Zahed Sarker
- Hannes Tschofenig
- Michael Tüxen
- Magnus Westerlund
Requirements

• The Design Team discussed before New Year what was perceived as the requirements to fulfill 3GPPs needs

• Presented at IETF 118 in TSVWG session:
  • [https://datatracker.ietf.org/meeting/118/materials/slides-118-tsvwg-sessb-3-tsvwg-design-team-to-set-requirements-for-dtlssctp](https://datatracker.ietf.org/meeting/118/materials/slides-118-tsvwg-sessb-3-tsvwg-design-team-to-set-requirements-for-dtlssctp)

• Further discussed and assigned importance:
The Proposals on the Table

• A: DTLS over SCTP based on RFC 6083 proposed by Ericsson
  • https://datatracker.ietf.org/doc/draft-ietf-tsvwg-dtls-over-sctp-bis/
  • https://datatracker.ietf.org/doc/draft-ietf-tsvwg-rfc4895-bis/

• B: DTLS Chunk alternative solution proposed by Ericsson
  • https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-dtls-chunk/
  • https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-dtls-handshake/

• C: Michael Tüxen’s and Hannes Tschofenig’s DTLS over SCTP proposal
  • https://datatracker.ietf.org/doc/draft-tuexen-tsvwg-rfc6083-bis/
  • https://datatracker.ietf.org/doc/draft-tuexen-tsvwg-sctp-ppid-frag/
  • https://datatracker.ietf.org/doc/draft-ietf-tsvwg-rfc4895-bis/
  • https://datatracker.ietf.org/doc/draft-tschofenig-tls-extended-key-update/
  • RFC 9261 for periodic Authentication
Analysis

• All three solution proposals meets the Design Team’s agreed technical requirements:

• The proposals differs in:
  • Some Technical Details and properties
  • IPR claims and impact on open source SCTP implementations
  • Expected time to complete the work in IETF
Completion Time

• A - DTLS over SCTP per Ericsson’s proposal:
  • All work is TSVWG internal
  • SCTP-AUTH needs to be completed
  • Specifications expected to be ready for publication request by end of 2024

• B - DTLS Chunk:
  • All work is TSVWG internal
  • Specifications expected to be ready for publication request by end of 2024

• C - DTLS over SCTP proposal by Tüxen et al
  • Dependent on adopting one technical function (key-update) into TLS WG
    • Key-update has general use not only for DTLS for SCTP
  • SCTP-AUTH needs to be completed
  • TSVWG documents expected to be ready for publication by end of 2024
  • Assuming adoption the Key Updated in TLS WG is expected time to be ready for publication request is at least 2 years
IPR

• A - DTLS over SCTP per Ericsson’s proposal:
  • Two IPR disclosures (RAND): https://datatracker.ietf.org/ipr/5195/
    https://datatracker.ietf.org/ipr/6218/

• B - DTLS Chunk:
  • draft-westerlund-tsvwg-sctp-dtls-chunk: https://datatracker.ietf.org/ipr/6219/
    • Defensive declaration with option of RAND (see disclosure)
  • draft-westerlund-tsvwg-sctp-dtls-handshake:
    • RAND license: https://datatracker.ietf.org/ipr/6220/

• C - DTLS over SCTP proposal by Tüxen et al
  • No IPR disclosures
IPR Implications

A. Two RAND license applying to implementation on top of a SCTP stack of DTLS for SCTP

B. Two different parts:
   1) Defensive Declaration with option of RAND on implementation that ends up inside SCTP stack, the license is attempting to not impact kernel open source
   2) A RAND license for the Rekeying implementation on top of the SCTP stack

C. Currently no IPR disclosure
A - DTLS over SCTP based on RFC 6083 proposed by Ericsson

• Depending on DTLS 1.3 features
  • DTLS Connection IDs
    • Could be engineered around with an DTLS record encapsulation layer

• Rekeying issue
  • Knowing when an old DTLS connection and its SCTP-AUTH key are no longer required
  • Interaction with SCTP-AUTH API that limits when key can be replaced

• Beyond SCTP-AUTH all on top of SCTP Stack

• Relies on SCTP stack for any replay protection

• Two crypto passes:
  • DTLS over ULP User Messages
  • SCTP-AUTH over SCTP Packet Chunks
B - DTLS Chunk alternative solution proposed by Ericsson

• One DTLS record per SCTP packet
  • Simple rekeying
  • Uses DTLS record size that are common in other DTLS applications
  • DTLS Replay protection prevents SCTP stack having to process replayed old packets
  • Single Crypto operation pass

• Encrypts SCTP protocol as well as ULP Data

• DTLS record processing integrated into SCTP stack
  • Kernel SCTP implementations require split DTLS implementation

• Maximum SCTP Payload MTU: 16384 bytes
  • Can be increased to 64 KB by DTLS Record size change (draft-mattsson-tls-super-jumbo-record-limit-00) (Optional improvement for large MTUs)
C - Michael Tüxen’s and Hannes Tschofenig’s DTLS over SCTP proposal

- Fragments ULP user messages into multiple SCTP messages
  - Requires in-order reliable delivery on streams
  - Enables I-Data like interleaving between streams of ULP user messages
  - Does not work with partial reliability messages (RFC 3758)

- Re-authentication based on RFC 9261
  - Cloudflare have implementations, none currently open source
  - Implementations are not particular large, one no more than ~300 lines

- Relies on SCTP stack for any replay protection

- Two crypto passes:
  - DTLS over ULP User Messages
  - SCTP-AUTH over SCTP Packet Chunks
Choosing a Solution

• The main choice is between timely completion and potentially IPR free
  • 3GPP has stressed in their LSes timely completion:
    • **RAN3**: ACTION: RAN3 asks IETF TSVWG group to take the above into account and expedite the discussion so that a solution which does not limit the maximum message size is selected as soon as possible.
    • **SA3**: ACTION: SA3 kindly asks IETF Transport Area Working Group (TSVWG) to take the above information into account and expedite the decision process so that a solution is ready by the envisioned time.

• For timely completion choose between type of SCTP stack impact:
  • DTLS Chunk: DTLS Chunk and potential split DTLS implementation
  • DTLS over SCTP per Ericsson: SCTP-AUTH and potentially improved API to solve rekeying ambiguities

• Else
  • DTLS over SCTP per Tüxen et al
<table>
<thead>
<tr>
<th>Options</th>
<th>Drafts</th>
<th>WG involved</th>
<th>IPRs</th>
<th>Time estimation</th>
<th>Implementation aspects</th>
</tr>
</thead>
</table>
Major dependencies on implementation on top of SCTP stack |
DTLS record processing integrated into SCTP stack  
SCTP kernel stack required  
Split DTLS implementation |
• [https://datatracker.ietf.org/doc/draft-tschohenig-tls-extended-key-update/](https://datatracker.ietf.org/doc/draft-tschohenig-tls-extended-key-update/)  
• RFC 9261 for periodic Authentication | TSVWG, TLS | 0 IPR disclosures | By end of 2024 at TSVWG  
By end of 2025 at TLS | Full solution can be implemented license free.  
Same split as A between SCTP stack and SSL/TLS libraries.  
Does not support partial reliability over 16384 bytes |
## Preferences from Participants in Design Team

<table>
<thead>
<tr>
<th>Party</th>
<th>Most Preferred</th>
<th>Least Preferred</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ericsson Participants</td>
<td>B</td>
<td>A</td>
<td>C is expected to take too long time</td>
</tr>
<tr>
<td>Nokia Participants</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>FreeBSD Maintainer</td>
<td>C</td>
<td></td>
<td>Could only implement half of B</td>
</tr>
<tr>
<td>Red Hat Linux and upstream SCTP stack maintainer</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS Implementer</td>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusions

• Does the WG agree that the requirements are acceptable?

• Can we close the Design Team?