DTLS over SCTP
RFC 6083 Update

draft-westerlund-tsvwg-dtls-over-sctp-bis-01

Magnus Westerlund, Ericsson
Claudio Porfiri, Ericsson
John Mattsson, Ericsson
Michael Tüxen, Münster University of Applied Sciences
Introduction

- 3GPP in 5G Networks uses DTLS over SCTP (RFC 6083) for securing several radio network application protocols.
- It has been realized that the F1, E1, Xn, NG-C interface protocols may send messages of sizes that exceed RFC 6083’s limitation of a single DTLS record (16383 bytes)
- 3GPP RAN2 has sent an LS asking TSVWG to address the issue [https://datatracker.ietf.org/liaison/1723/](https://datatracker.ietf.org/liaison/1723/)
- 3GPP would prefer a general solution to not having to address the issue in each protocol individually

- RFC 6083 maps a user message to single DTLS record
  - User message sizes a limited by DTLS record sizes, which is too small
- RFC 6083 security requirements are also outdated
  - DTLS 1.0 (TLS 1.1 based)
  - SHA-1 in SCTP-AUTH (RFC 4895)
Proposal

- Replace RFC 6083 with an updated specification
- Define a secure fragmentation mechanism
- Updated Security Requirements
  - DTLS 1.2 or DTLS 1.3
  - Require SHA-256 support for SCTP-AUTH
- Signaling of supported message sizes
- Defined as SCTP Adaptation Layer
  - Handshake indication
  - Recommend support of I-DATA (RFC 8260)
  - Clarify DTLS 1.2 Renegotiation to minimize impact from rekeying

Plain Text

User Message

Fragmentation

m1  m2  m3  m4

DTLS Protect Operation

m1' m2' m3' m4'

Protected User Message

SCTP Authentication

SCTP Transmission
SCTP Authentication Reliance

- Like RFC 6083 this is dependent on SCTP-AUTH to achieve security properties:
  - Combined with SCTP's reordering provide Replay Protection
    - Replaying an SCTP packet will not impact protected user messages
  - SCTP ensuring DTLS record order in each protected user message
  - SCTP AUTH ensures that third party can not impact the order of the DTLS records being received, thus integrity of user message is preserved
Open Issues

- DTLS 1.3 and rekeying for long lived flows
  - DTLS 1.3 do not support renegotiation
  - No post-handshake server authentication, Diffie-Hellman, and exporter_secret update possible
  - Negative impact on security for long lived flows
  - Started discussion in TLS WG
- With SCTP Adaptation Layer signaling we can require DTLS to be used for all User Messages
  - StartTLS will not work under these restrictions
- Specify handling of partially delivered protected user messages
  - Relevant when partial reliability is used
- How to deal with socket API changes related to RFC 4895 to allow usage of SCTP AUTH as required by this specification?
Going Forward

- Request adoption as WG Item
  - RFC 6083 needs update
  - Resolve message length restriction
  - Update security algorithm requirements
  - 3GPP needs a solution, preferably in Rel-17 timeframe (March 2022)

- Discussion of open issues on mailing list
- Resolve some editorial
- Source, Pull Requests and Tracking issues at: https://github.com/gloinul/draft-westerlund-tsvwg-dtls-over-sctp-bis