DTLS/SCTP

Michael Tüxen
tuexen@fh-muenster.de

TLS/SCTP

- Is defined in RFC 3436.
- Hard to implement in OpenSSL.
- Has serious limitations:
  - It needs an SSL connection per bidirectional stream.
  - Does not support unordered delivery.
  - Does not support PR-SCTP as defined in RFC 3758.

Objectives for DTLS/SCTP

- Overcome the limitations of TLS/SCTP, especially support all features of SCTP.
- Easy to implement in OpenSSL.
- Reuse as much as possible.
- Do not change (security) protocols, only use them.

Why simple DTLS/SCTP does not work

- UDP/DCCP is completely unreliable, therefore it is OK for DTLS to drop user messages.
- An attacker can drop DATA chunk and replace them by SACKs/FORWARD-TSN and make both sides happy. This can only be avoided at the SCTP layer. SCTP-AUTH is used for this.

SCTP AUTH

- Enables a receiver to make sure that a received chunk is really sent from the same entity which was involved during association setup.
- It exchanges random numbers to get an per end-point pair shared key.
- Can make use of multiple shared secrets.
- No built-in method of establishing the secrets.

How does it work?

- SCTP-AUTH is used to authenticate DATA, SACK and FORWARD-TSN chunks.
- SCTP-AUTH uses a shared secret computed by the DTLS.
- DTLS is not allowed to discard messages.
- DTLS control messages are transported reliably by SCTP.

DTLS/SCTP

- Is described in draft-tuexen-dtls-for-sctp-00.txt
- Needs to get the shared secret for SCTP-AUTH from DTLS.
- The only limitation still available is the size of DTLS user messages…
- Comments are really appreciated!