Authenticated Chunks for SCTP

draft-tuexen-sctp-auth-chunk-03.txt

Eric Rescorla

Peter Lei

Randall Stewart

Michael Tüxen

SCTP-AUTH and ADDIP

- Using the ADDIP extension it is possible for an attacker to take over an association.
- SCTP-AUTH provides a way to proof that chunks are sent by the same end point as before.
- ADDIP MUST only be used in combination with SCTP-AUTH.

Key establishment

- During the association setup both endpoints exchange 32 byte random numbers.
- There might be preconfigured shared key between the end points.
- The shared key used is the concatenation of the preconfigured array and the exchanged random numbers.

AUTH chunk

- A new control chunk (AUTH chunk) is defined which contains the result of an HMAC computation.
- The HMAC is computed on (a zeroed) AUTH chunk and the chunks after the the AUTH chunk.
- If the HMAC verification fails at the receiver all chunks after the AUTH chunk MUST be discarded.

Additional functionality

- The chunks that an endpoint requires to be authenticated are ‘negotiated’ on association setup.
- Some chunks can not be authenticated.
- The hash algorithm for the HMAC computation needs to be negotiable.

Limitation

- An on path attacker which captures the association setup can take it over anytime if no preconfigured shared key is used.
- But this is not different if only RFC 2960 is used.