Authenticated Chunks for Stream Control Transmission Protocol (SCTP) draft-tuexen-sctp-auth-chunk-00.txt

Michael Tüxen (tuexen@fh-muenster.de)

Randall Stewart (rrs@cisco.com)

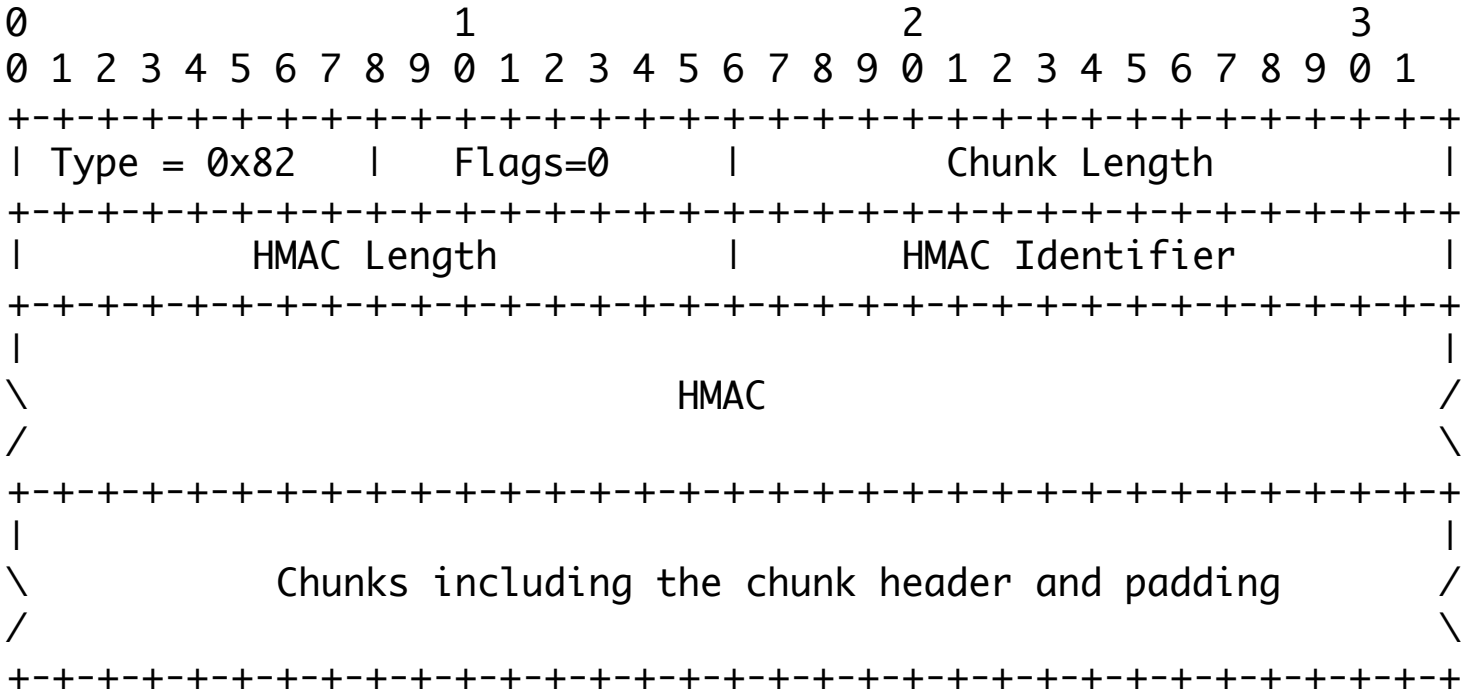
Why is the extension needed?

- In the ADD-IP extension the ASCONF chunks are 'only' protected by some long living data transmitted in plain text.
- TLS can not be used to authenticate control chunks.
- IPSec can only be used to authenticate all packets of an association and re-keying is required on an address change.

How does is work?

- Similar to the TCP MD5 Signature Option (RFC 2385).
- The chunks being authenticated are put into a new chunk (AUTH-chunk) and an HMAC (RFC 2104) is computed.
- The AUTH chunk also contains an identifier for the message digest algorithm. Currently SHA-1 and MD-5 are supported.
- Whenever something goes wrong, the chunks are discarded.

The chunk format



How can it be used?

- Configure for both SCTP-endpoints the list of chunks which needs to be authenticated.
- Configure for both SCTP-endpoints a shared key.
- This can be done for example:
  - Manually
  - By using TLS over SCTP (not yet specified)

Security considerations

- Downgrade attacks.
- Replay attacks.

What needs to be done?

- Make the security considerations section better.
- Should we add some mechanism for establishing a shared key at the SCTP layer?
- Should we specify some mechanism for establishing a shared key using TLS?
- Incorporate suggestions from the list.