RFC 4895bis: SCTP Authentication

draft-ietf-tsvwg-rfc4895-bis-03

Michael Tüxen (tuexen@fh-muenster.de)
Randall Stewart (randall@lakerest.net)
Peter Lei (peterlei@netflix.com)
Hannes Tschofenig (hannes.tschofenig@gmx.net)

Original Scope

- Incorporate relevant changes from draft-nagesh-sctp-auth-4895bis-00
- Address two security issues reported by Ericsson:
  - Use direction dependent keys to mitigate reflection attacks.
  - Don’t use different HMAC algorithms with the same keys.
- Generalize HMAC to MAC.
- Add more algorithms, potentially retire HMAC-SHA-1.
- Add socket API considerations for improved control of the SCTP AUTH usage.

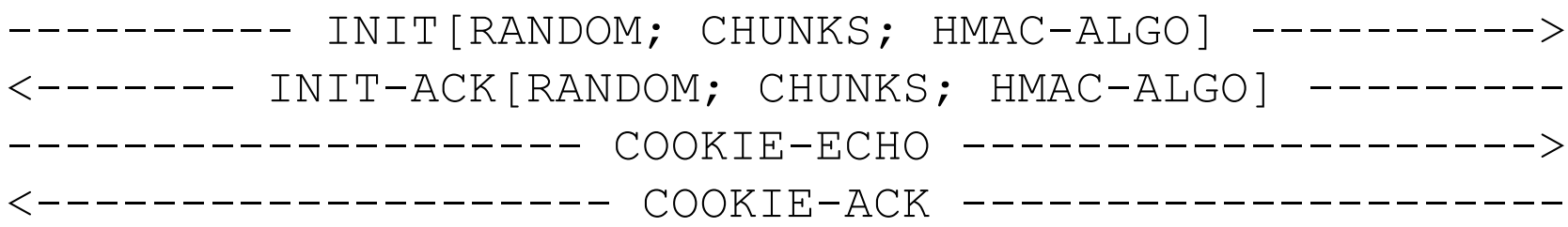
Status (I)

- draft-tuexen-tsvwg-rfc4895-bis-00
  Submit RFC 4895 as an ID.
- draft-tuexen-tsvwg-rfc4895-bis-01
  Update to xmlv3.
- draft-tuexen-tsvwg-rfc4895-bis-02
  Wordsmithing and updating references.
- draft-tuexen-tsvwg-rfc4895-bis-03
  Minor editorial change.
- draft-tuexen-tsvwg-rfc4895-bis-04
  Add socket API related updates required for DTLS/SCTP.
- draft-tuexen-tsvwg-rfc4895-bis-05
  Remove ekr from list of authors, improve socket API.
- draft-tuexen-tsvwg-rfc4895-bis-06
  Update Acknowledgements.

Status (II)

- draft-tuexen-tsvwg-rfc4895-bis-00
  Same as draft-tuexen-tsvwg-rfc4895-bis-06.
- draft-tuexen-tsvwg-rfc4895-bis-01
  Incorporate draft-nagesh-sctp-auth-4895bis-00, editorial changes, update IANA section.
- draft-tuexen-tsvwg-rfc4895-bis-02
  Introduce directional keys.
- draft-tuexen-tsvwg-rfc4895-bis-03
  Deprecate Unsupported HMAC Identifier Error Cause, various editorial improvements (thanks to Timo Völker!)

SCTP AUTH Handshake



Legacy Mode

- Allows to communicate with RFC 4895 implementations.
- Must be enabled by the upper layer, disabled by default.
- If enabled, the HMAC ALGO parameter sent contains the connectionless SHA-1 algorithm and possibly the connectionless SHA-256 algorithm.
- Will be used only if the peer only supports directionless SHA-1 or directionless SHA-256.

Proposal 1

- Shorten the CHUNKS parameter in the case of all chunks, which can the authenticated, needs to be authenticated.
- Proposed for DTLS over SCTP.
- Instead of listing in the CHUNKS parameter all chunks except INIT, INIT-ACK, SHUTDOWN COMPLETE, and AUTH, don’t list any.
- This is only supported, if the peer can not be in legacy mode.

Proposal 2

- Improve replay protection:
  - Add 64-bit sequence number to the AUTH chunk.
  - Incremented by one for each AUTH chunk.
  - The receiver uses a sliding window to enforce, that each chunks protected by an AUTH chunks are accepted at most once. Like the replay protection in IPSec.
- This is only supported, if the peer can not be in legacy mode.

Next Steps

- Integrate Proposal 1 and 2 is supported by the WG.
- Use a formula-based description instead of a text based one.
- Generalize in the text HMAC to MAC.
- Add more algorithms. Which ones?
- Address comments already received and all upcoming comments.