RFC 4895bis: SCTP Authentication

draft-tuexen-tsvwg-rfc4895-bis-06

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

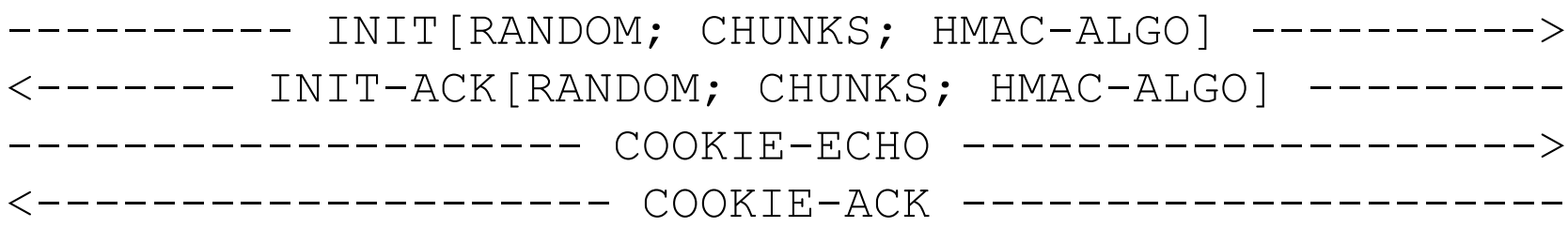
Motivation

- 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.
- Add more algorithms, potentially retire HMAC-SHA-1.
- Incorporate relevant changes from draft-nagesh-sctp-auth-4895bis-00
- Add socket API considerations allowing applications to query which algorithms are used for sending and to get notified about changes of parameters when receiving.

Status

- 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.

SCTP AUTH Handshake



How to Differentiate Directions?

- Can’t be done based on client/server role like in (D)TLS.
- key_vector = RANDOM|CHUNKS|HMAC_ALGO
- The RANDOM parameter contains a 32-byte random number.
- Base the role on which side selected the smaller or larger key_vector.
- How to handle that both key_vectors are the same:
  - Can be avoided easily in a client/server situation.
  - Might result in an association setup failure peer to peer situation with a small likelihood. Redo the handshake without involving the upper layer.

Next Steps

- Working group adoption?
- Address
  - Comments sent my Magnus to tsvwg@ietf.org.
  - all issues listed in the motivation.
  - anything else required for DTLS/SCTP.
  - any additional feedback.