RFC 4895bis: SCTP Authentication

draft-tuexen-tsvwg-rfc4895-bis-02

Michael Tüxen (tuexen@fh-muenster.de)
Randall Stewart (randall@lakerest.net)
Peter Lei (peterlei@Netflix.com)
Eric Rescorla (ekr@rtfm.com)

Motivation

- Incorporate relevant changes from draft-nagesh-sctp-auth-4895bis-00
- Add more algorithms, potentially retire HMAC-SHA-1.
- Add socket API considerations allowing applications to query which algorithms are used for sending and to get notified about changes of parameters when receiving.
- Use part of the common header in the computation of the MAC to mitigate reflection attacks. Recently brought up by Ericsson.
- Improve handling of using direction specific algorithms (using key derivation, for example). Recently brought up by Ericsson.

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.

Next Steps

- Incorporate any additional feedback.
- Working group adoption?