RFC 4895bis: SCTP Authentication

draft-tuexen-tsvwg-rfc4895-bis-03

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

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

• Use the verification tags.
• Possibly use the port numbers. This breaks NAPT, but NAPT for SCTP is a bad idea anyway.
• Different verification tags can be enforced in the handshake, when not handling an INIT collision. Is that an acceptable idea?
• Fail the collision case of identical initiate tags?
Next Steps

• Address
  – all issues listed in the motivation.
  – anything else required for DTLS/SCTP.
  – anything required to be done by the authors before considered for WG adoption.
  – any additional feedback.