SCTP-AUTH Security Issues

IETF 115, TSVWG, John Preuß Mattsson

https://www.flickr.com/photos/aquamech-utah/24445486463/in/photostream/

Required Properties for Modern Security Protocols

1. **Strong Data confidentiality (against active attackers)**
2. **Strong Data origin authentication**
3. **Strong Data integrity protection**

Often bundled together as "integrity"

4. **Strong Data replay protection**
5. **High availability**

— Strong: Offline attacks should be as computationally infeasible as breaking AES, SHA, ...
Slightly lower security can be allowed for online attacks that requires sending many packets.

— Data refers to user messages not internal SCTP stuff like data chunks or SCTP packets.

— Availability means that services and information must be available when needed. Can refer to the SCTP transport service or log files. Not as easy to define mathematically as property 1-4. Must not be easier than expected to affect availability.

— Security requirements has increased drastically. Most modern deployments like 5G require all five properties above. Interfaces in the 5G core uses IPsec, (D)TLS, and MACsec with 128-bit integrity tags.

Five SCTP-AUTH Security Issues

1. **Reflection of authenticated data chunks**

   — As SCTP-AUTH endpoint shared secrets are not directional, an on-path attacker* can reflect authenticated data chunks back to the sender.

   *The on-path attacker must able to read (but not write) on-path, i.e., might not be able to otherwise change or block SCTP packets.

   — For a reflected data chunk to be accepted, the TSN, Stream Identifier, and Stream Sequence Number need to "match".

   — **Worst case:** If user messages are large (more chunks than the difference in Initial TSNs), the attack can trivially be done after $0\text{-}2^{31}$ chunks as the TSN reaches the peer's Initial TSN.

   — An attacker might denial-of-service the association to force endpoints to setup a new association and hope it has a smaller difference between the Initial TSNs.

   — Accepted reflected data chunks result in that the whole or part of a user message is reflected. A rejected reflected data chunks might result in an error condition.

   — Breaks data/chunk origin authentication and data integrity protection. Weakens confidentiality in protocols relying on SCTP-AUTH for data integrity protection.

Five SCTP-AUTH Security Issues

2. Replay of authenticated data chunks

- After the 2^{32} data chunks the TSN reaches the Initial TSN and an on-path attacker* can replay authenticated data chunks.
- For a replayed data chunk to be accepted, the TSN, Stream Identifier, and Stream Sequence Number need to "match".
- **Worst case:** If user messages are large (more chunks than 2^32), the attack can trivially be done after 2^{32} chunks when the TSN reaches the Initial TSN.
- Accepted replayed data chunks result in that the whole or part of a user message is replayed. A rejected replayed data chunks might result in an error condition.
- Breaks data/chunk replay protection and data integrity protection. Weakens confidentiality in protocols relying on SCTP-AUTH for data integrity protection.

Five SCTP-AUTH Security Issues

3. **Single key used with different HMAC algorithms**

   — Theoretical issue. This breaks the security proofs of the individual algorithms. Doing this is e.g., MUST NOT in TLS 1.3 and SHOULD NOT in COSE. Likely not a practical issue with the current HMAC algorithms.

4. **Reflection of authenticated control chunks**

   — As SCTP-AUTH endpoint shared secrets are not directional, an on-path attacker* can reflect authenticated control chunks back to the sender.

   — Many control chunks are easy to reflect as there is no need to "match" the current TSN. ERROR can be trivially be reflected. Reflected SACK would lead to packet loss, missing data that is not delivered, and an inconsistent state. Reflected HEARTBEAT ACK might lead to the association being aborted.

   — This is an attack on availability by disrupting the service (aborted association or missing data) or the logs.

5. **Replay of authenticated control chunks**

   — Similar to 4. Reflected ERROR is worse then replayed ERROR.

Promised properties in RFC 4895, RFC 6083, draft-ietf-tsvwg-dtls-over-sctp-bis, and 3GPP TS 33.501

RFC 4895:

> *"control and data chunks that are placed after the AUTH chunk in the packet are sent in an authenticated way "*
>
> *"even a true man in the middle cannot inject chunks, which are required to be authenticated"*
>
> *"a method of proving that an SCTP chunk(s) was really sent by the original peer"*
>
> *"Because SCTP already has a built-in mechanism that handles the reception of duplicated chunks, the presented solution makes use of this functionality and does not provide a method to avoid replay attacks by itself."*
>
> SCTP-AUTH seems to promise chunk integrity protection, chunk origin authentication, and chunk replay protection. Combined with reliable transport.

RFC 6458:

> *"[RFC4895] defines an extension to authenticate SCTP messages"*

RFC 6083:

> Does not give any properties, just says that DTLS and SCTP-AUTH is used and that DTLS replay protection is not used.

3GPP TS 33.501:

> *"In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection."*

draft-ietf-tsvwg-dtls-over-sctp-bis-05:

> *"This specification provides mutual authentication of endpoints, data confidentiality, data origin authentication, data integrity protection, and data replay protection of user messages"*

Impact of Security Issues on RFC 4895, RFC 6083, draft-ietf-tsvwg-dtls-over-sctp-bis

RFC 4985:

RFC 4985 (SCTP-AUTH) does not offer chunk origin authentication, chunk replay protection, data origin authentication, data integrity protection, or data replay protection. Confidentiality protocols relying on SCTP-AUTH for data integrity protection only offers confidentiality against passive attackers (confidentiality against active attackers requires integrity). RFC 4985 is vulnerable to attacks on availability.

RFC 6083:

RFC 6083 does not offer data replay protection. As RFC 6083 uses a single DTLS record per user message and uses directional keys, RFC 6083 offers data integrity protection, data origin authentication, and data confidentiality against active attackers. The reflection and replay attacks becomes attacks on availability instead. RFC 6083 is vulnerable to attacks on availability.

draft-ietf-tsvwg-dtls-over-sctp-bis

-04 does not offer data origin authentication, data integrity protection, data replay protection, or data confidentiality against active attackers. Vulnerable to attacks on availability.

-05 offers data confidentiality against active attackers, data origin authentication, data integrity protection, and data replay protection. Requires changes to SCTP-AUTH and API. Vulnerable to attacks on availability.

A lot of the behaviour upon receiving reflected or replayed chunks are implementation specific.