Analysis of Middlebox Interactions for Signaling Protocol Communication along the Media Path

draft-sipping-stuckerm-media-path-middleboxes-00

Brian Stucker

Hannes Tschofenig
References

• [Framework]
  Framework for Establishing an SRTP Security Context using DTLS
  (draft-ietf-sip-dtls-srtp-framework-00)

• [Middleboxes]
  Analysis of Middlebox Interactions for Signaling Protocol
  Communication along the Media Path
  (draft-sipping-stucker-media-path-middleboxes-00)

• [DTLS-SRTP-Prot]
  Datagram Transport Layer Security (DTLS) Extension to Establish
  Keys for Secure Real-time Transport Protocol (SRTP)
  (draft-ietf-avt-dtls-srtp-01)
Middleboxes in the Media Path

- Functions of the middleboxes (cf. [Middleboxes]):
  - gating/pinholing: block all flows that are not allocated by the MIDCOM-agent
  - NAT/media relay: For a bidirectional flow A<->B, allocate a pair of transport addresses, one representing B towards A, one representing A towards B, and relay traffic accordingly
- Focus of the presentation is on firewalls.
Example Message Flow from [Framework]

- INVITE (offer) → INVITE(offer)
- DTLS – Hello
- DTLS – Hello
- DTLS – Finished
- Media
- DTLS – Finished
- 200 OK → 200 OK
- Media
- ACK → ACK
Recommendations

• [Middleboxes] goes beyond a problem description.

• It aims to make recommendations (to trigger discussions)
  – Details need to be investigated
  – Other solution approaches also possible
REC #1

• Ensure that a mechanism exists that causes both endpoints to send at least one packet in the forward direction as part of, or prior to, the handshake process.
REC #2

- Allow a nominal amount of traffic to be exchanged between endpoints to enable completion of media path signaling prior to the session being established.
REC #3

• The failure to complete signaling on the media path should not automatically cause the session establishment to fail unless explicitly specified by one or more endpoints.
Next Steps

• Waiting for feedback from the group on how we should proceed