DTLS-SRTP Handling in SIP B2BUAs

draft-ram-straw-b2bua-dtls-srtp

IETF-90

Toronto, July 25, 2014

Presenter: Lorenzo Miniero

Authors: Ram Mohan, Tirumaleswar Reddy,
Gonzalo Salgueiro, Victor Pascual

Background

- DTLS-SRTP is used to secure media
- Certificate fingerprint exchange in SDP for mutual authentication
- Need for B2BUA to handle DTLS-SRTP

DTLS-SRTP Handling in SIP B2BUA

- This draft defines the behavior B2BUA must follow to handle DTLS-SRTP in following modes:
  - Media Relay
  - Media Aware
  - Media Termination

Media Relay

- Forwards packets without inspection or modification
- Only modifies the L3 and L4 headers
- It MUST forward the received certificate fingerprint without any modifications

Media Aware

- Media Aware only modifies the RTP header
- Terminates the DTLS connection and acts as a DTLS proxy
  - Changes the certificate fingerprint and signals its own fingerprint
  - Decrypts and re-encrypts the payload

Media Termination

- Media terminator modifies the payload
- Terminates the DTLS connection, acts as a DTLS proxy
  - Changes the certificate fingerprint and signals its own fingerprint
  - Decrypts and re-encrypts the payload

Media Plane B2BUA to Handle NAT

- NAT between UA and B2BUA
- NAT could drop unsolicited incoming packets
- UA in passive mode must send some packets (STUN, RTP, etc.) so as to receive the incoming ClientHello packet from B2BUA
- Restart DTLS handshake after answer is received

Next Steps

- Adopt as WG document
- Need additional reviews