DTLS-SRTP Key Transport

AVT Working Group

draft-wing-avt-dtls-srtp-key-transport-01

Dan Wing, dwing@cisco.com
Key Transport Overview

- IETF68 (Prague), RTPSEC BoF selected DTLS-SRTP as the preferred SRTP keying mechanism
- Only unicast, point-to-point was in scope

- DTLS-SRTP Key Transport allows efficient SRTP operation for:
  - Unicast audio and video conferencing
  - Multicast
  - Voicemail storage and retrieval
GDOI-SRTP and DTLS-SRTP-Key-Transport

- MSEC has Group SRTP Keying
  - draft-ietf-msec-gdoi-srtp

Differences

<table>
<thead>
<tr>
<th>MSEC GDOI-SRTP</th>
<th>DTLS-SRTP-Key-Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy to remove group member</td>
<td>Extension to already-required SRTP keying mechanism</td>
</tr>
<tr>
<td>Easy to change SRTP key</td>
<td></td>
</tr>
</tbody>
</table>
Changes in -01

• Incorporated feedback from Vancouver
  – Now better aligned with RTP Topologies (RFC5117)
  – Added voicemail storage/retrieval scenario

• New multicast scenario
  – Separate MSEC presentation

• Additional key transport messages
  – delete_srtp_key, your_new_srtp_key
Scenarios
Point to Multipoint using RFC3550 Mixer Model

- Transport one SRTP key, inside of the per-listener DTLS session, to legitimate listeners

![Diagram](image)
Point to Multipoint using Video Switching MCUs

- Transport speaker’s keys to listeners
- SRTP packets not encrypted/decrypted by switcher
Point to Multipoint using Multicast

1. Each listener establishes unicast DTLS-SRTP session with speaker
2. Speaker uses DTLS-SRTP Key Transport to tell every listener the same SRTP key
3. (not shown) SRTP packets multicasted

Listener 1
Listener 2
Listener 3

speaker

DTLS-SRTP, transport speaker’s SRTP key=A
Voicemail Storage and Retrieval

1. SRTP, and its SRTP key, are saved to voicemail server
   - Speaker doesn’t need DTLS-SRTP Key Transport
   - Voicemail server doesn’t need to decrypt SRTP

2. Later, voicemail is retrieved using DTLS-SRTP
   - Voicemail server doesn’t need to encrypt SRTP
DTLS-SRTP Key Transport

Questions

draft-wing-avt-dtls-srtp-key-transport-01

Dan Wing, dwing@cisco.com