RTPSEC BoF

IETF 68, Prague

Chairs:
Russ Housley, housley@vigilsec.com
Dan Wing, dwing@cisco.com
Agenda

15:20 Agenda bash (Chairs)

15:20 Goals of this BoF (Jennings, 5)

15:25 Summary of Montreal discussion (Wing, 5)

15:30 Status of MMUSIC SDP negotiation work (Andreasen, 10)

15:40 Requirements Evaluation (Wing, 15)
Intrinsic Features of DTLS-SRTP, MIKEYv2, ZRTP
Path Forward

15:55 DTLS-SRTP (Rescorla, 15)

16:10 MIKEYv2 (Dondeti, 15)

16:25 ZRTP (Zimmermann, 15)

16:40 Discussion (All, 35)

17:15 Hums (Chairs/AD, 5)
Status

Montreal BoF
Montreal BoF Summary

• Presentations
  – Best-Effort SRTP (Johnston)
  – Keying in Media versus Signaling Path (Dondeti)
  – Shared key conferencing (McGrew)

• Top Priorities:
  – Solve keying for point-to-point unicast
  – Make it secure with forking and retargeting
  – Key exchange in media path

• Requirements: draft-wing-media-security-requirements
Analysis of Current Proposals
Source Material

• Requirements:
  – draft-wing-media-security-requirements-01
• DTLS-SRTP
  – draft-mcgrew-tls-srtp-01
  – draft-fischl-mmusic-sdp-dtls-02
  – draft-fischl-sipping-media-dtls-02
• ZRTP
  – draft-zimmermann-avt-zrtp-03
• MIKEYv2
  – draft-dondeti-msec-rtpsec-mikeyv2-01
## Summary of Differences

<table>
<thead>
<tr>
<th>Level</th>
<th>Requirement</th>
<th>DTLS</th>
<th>MIKEYv2</th>
<th>ZRTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>R2: mixed SRTP/RTP w/forking and w/retargeting</td>
<td>Via cap-neg</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>M</td>
<td>R9: multiple RFC3711 cipher suites</td>
<td>Yes</td>
<td>?</td>
<td>Yes</td>
</tr>
<tr>
<td>S</td>
<td>R10: DH performance</td>
<td>TLS session resumption</td>
<td>To be spec’d</td>
<td>Preshared mode</td>
</tr>
<tr>
<td>S</td>
<td>R12: FIPS-140-2</td>
<td>Yes</td>
<td>Unknown</td>
<td>w/ some effort</td>
</tr>
<tr>
<td>M</td>
<td>R11a: No 3rd party certificates</td>
<td>Meets</td>
<td>To be spec’d</td>
<td>Meets</td>
</tr>
<tr>
<td>S</td>
<td>R11b: use shared authentication infrastructure</td>
<td>Yes</td>
<td>Yes</td>
<td>Probably (signed SAS)</td>
</tr>
<tr>
<td>S</td>
<td>R13: Associate signaling/media</td>
<td>a=fingerprint</td>
<td>To be spec’d</td>
<td>a=zrtp-zid</td>
</tr>
<tr>
<td>S</td>
<td>R14: Upgrade from RTP to SRTP</td>
<td>Via cap-neg</td>
<td>Via cap-neg</td>
<td>Yes, w/ probe and re-Invite</td>
</tr>
<tr>
<td>S</td>
<td>R15: Active Attacks (needs further study)</td>
<td>Yes, a=fingerprint</td>
<td>To be spec’d</td>
<td>a=zrtp-zid, a=zrtp-sas</td>
</tr>
<tr>
<td>S</td>
<td>R16: signal in SIP and media</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, but not required</td>
</tr>
<tr>
<td>S</td>
<td>R21: VoIP signaling agility *</td>
<td>IWF cooperation or probe&amp;SAS</td>
<td>No, IWF cooperation</td>
<td>Yes, w/ probe</td>
</tr>
</tbody>
</table>
R2: mixed RTP and SRTP with forking and with retargeting

- DTLS-SRTP: Via mmusic-sdp-capability-negotiation (in progress)
- MIKEYv2: No
- ZRTP: Yes
R9: Multiple RFC3711 Cipher Suite Upgrades

- DTLS-SRTP: Yes
- MIKEYv2: ?
- ZRTP: Yes
R10: DH Performance

- DTLS-SRTP: session resumption for multiple streams and for new session with previous endpoint
- MIKEYv2: To be specified
  - Considering MIKEY-PSK
- ZRTP: preshared mode for multiple streams and for new session with previous endpoint
R11a: MUST NOT require 3rd-party certificates

- DTLS-SRTP: Meets requirement
- MIKEYv2: To be specified
  - Carry raw RSA keys
- ZRTP: Meets requirement
R11b: Be able to use shared authentication infrastructure

- DTLS-SRTP: Yes
  - certificates [RFC4346]
  - kerberos [RFC2712]
  - pre-shared key [RFC4279][RFC4785]

- MIKEYv2: Yes

- ZRTP: Probably using its signed SAS
  - Underspecified in -03
R12: FIPS-140-2

- DTLS-SRTP: Yes
  - TLS meets FIPS-140-2, DTLS is derived from TLS
- MIKEYv2: Unknown
- ZRTP: With some effort
  - Specification being adjusted to comply
  - Uses allowable algorithms
R13: Associate Signaling with Media

- DTLS-SRTP: Yes, a=fingerprint
- MIKEYv2: To be specified
- ZRTP: Yes, a=zrtp-zid
R14: Start with RTP, upgrade to SRTP

- DTLS-SRTP: Via mmusic-sdp-capability-negotiation (in progress)
- MIKEYv2: Via mmusic-sdp-capability-negotiation (in progress)
- ZRTP: Yes, with probe and re-Invite
R15: Consider active attacks, including DoS

- DTLS-SRTP: Yes
- MIKEYv2: To be spec’d
- ZRTP: Yes, if a=zrtp-zid and a=zrtp-sas are used
R16: SIP Signaling and Media Path

- DTLS-SRTP: Yes
- MIKEYv2: Yes
- ZRTP: Yes, although not required for operation
R21: Call Signaling Agility (SIP, Jabber, H.323)

- DTLS-SRTP:
  - Requires interworking function (IWF) cooperation or
  - Probing* and SAS (underspecified)
- MIKEYv2: No, requires interworking function (IWF) cooperation
- ZRTP: Yes
  - media probing obviates need for IWF cooperation

* Probing is possible with DTLS-SRTP;
  reference §3.6.2.1 of draft-mcgrew-tls-srtp-02
Intrinsic Features and Steps to Become a Standard

High-Level “Big Differences” in the three approaches
DTLS-SRTP

Intrinsic Features
• Based on DTLS which is based on TLS
  – TLS cipher suites
  – FIPS-140-2 compliance
• Certificates on endpoints
• Fingerprint in SDP of initial Invite
• 4 messages to establish

Standardization Steps
• mmusic-cap-neg
MIKEYv2

Intrinsic Features

• Re-uses MIKEY payloads
• Includes group keying support
• 2 messages to establish

Standardization Steps

• ?
ZRTP

**Intrinsic Features**
- Hash commitment
- Perfect forward secrecy
- Short Authentication String (SAS)
- SAS in SDP of re-Invite
- Deployed today
- 4 messages to establish, 7 total

**Standardization Steps**
- Peer review of protocol
- SAS signing
Key Exchange Mechanisms

DTLS-SRTP, Eric Rescorla
MIKEYv2, Lakshminath Dondeti
ZRTP, Phil Zimmermann
RTPSEC Discussion