SRTP EKT Update
draft-ietf-avtcore-srtp-ekt-02

Dan Wing
dwing@cisco.com

IETF89 London, March 3, 2014

EKT Changes from -01 to -02

- Review comments by Michael Peck, John Mattsson, and Magnus Westerlund
- MKI prohibited with EKT
  - Duplicates EKT function
- SRTCP compound packet problem (next slide)
- Clarify EKT is negotiated during call setup
- SRTP master keys: random, never shared
- Removed alternate EKT host (a=dtls-srtp-host)
  - If interest, can be separate document

SRTCP Compound Packet

- RTP mixer is encouraged to optimize RTCP
  - Section 6.1 of RFC3550
- Complicates EKT at end of RTCP packet
  - RTCP SSRC doesn't match EKT SSRC
  - EKT-unaware RTP mixer
  - Multiple RTCP packets with EKT

- Need ability to send EKT over RTCP
  - one-way audio
- Resolution: Document problem in EKT, and encourage sending EKT over SRTP.

SRTP EKT Update
draft-ietf-avtcore-srtp-ekt-02

Dan Wing

dwing@cisco.com

Text for RTCP compound packets

"These compound SRTCP packets might have an SSRC that does not match the EKT SSRC. There is no good solution to handling these SRTCP compound packets, except hoping the mixer or translator round robin between the SSRCs, but this would require several SRTCP packets, further delaying receipt of EKT over RTCP. This impact of RTP translators and mixers, and the inability to realibly determine an RTP translator or mixer might be involved in an RTP session, provides further incentive to send EKT over RTP."