DTLS-SRTP Key Transport ("KTR")

AVT Working Group

draft-wing-avt-dtls-srtp-key-transport-02

Dan Wing, dwing@cisco.com
Key Transport Overview

- DTLS-SRTP Key Transport allows efficient SRTP operation for:
  - Unicast audio and video conferencing
  - Multicast
Changes in -02

• Incorporated feedback from Philadelphia
  – Removed voicemail storage/retrieval scenario
  – Described relationship with EKT
• Technical improvements
  – Nascent LKH (Logical Key Hierarchy) support
  – Removed ‘your_new_key’ primitive
    • Too easy to create two-time pad
• Text
  – Describe Join/Leave scenarios for Speakers and Listeners
  – New scenario: Interworking with Security Descriptions (SDESC)
Logical Key Hierarchy (LKH) 
and 
Interworking with SDESC
Logical Key Hierarchy: Use Case

• Need new SRTP key when a listener joins or leaves
• With normal DTLS-SRTP, new SRTP key is encrypted $N$ times for $N$ active listeners
  – Takes time and CPU cycles

• LKH allows new SRTP key to be encrypted 1 time for $N$ listeners
• Design consideration: how to deliver that new key to the listeners?

LKH: RFC2627
Logical Key Hierarchy: SRTP Design Considerations (not in draft)

1. DTLS-SRTP-KTR with EKT for re-keying
   - Complex
   - EKT with video switching scenario
     • EKT uses RTCP messages with SSRCs
     • video switcher has to synthesize its own SSRC
     • Video switcher isn’t an RTP endpoint, so can it send RTCP?

2. Invent new DTLS-SRTP content-type to send LKH message
   - keeps SRTP keying in DTLS-SRTP (rather than in EKT/RTCP messages)
   - Could do this similar to DTLS-SRTP’s ‘application_data’ content type

• Is LKH useful enough to standardize?
Security Descriptions: Background and Requirement

• Deployed in many IP PBXs today
• Might be 3GPP’s direction
  – We do not yet know for sure

• Need to interwork DTLS-SRTP with Security Descriptions
  – While waiting for upgrades to DTLS-SRTP
• Problem: CPU-intensive to interwork

Security Descriptions: RFC4568
Without Key-Transport:
CPU intensive in one direction

Security Descriptions endpoint

SBC

DTLS-SRTP endpoint

a=crypto=AAA

a=crypto=BBB

SRTP packet, key=AAA

DTLS-SRTP handshake

Key=BBB, CCC

SRTP packet, key=CCC

SRTP packet, key=BBB

(Authenticate, Decrypt, Encrypt, HMAC)

(do nothing)
With Key-Transport:
CPU efficient

Security Descriptions endpoint

SBC

DTLS-SRTP-KTR endpoint

a=crypto=AAA

a=crypto=BBB

SRTP packet, key=AAA

SRTP packet, key=AAA

(do nothing)

(new_srtp_key=AAA)

SRTP packet, key=AAA

SRTP packet, key=BBB

(do nothing)

SRTP packet, key=BBB

Key=BBB, CCC
DTLS-SRTP Key Transport ("KTR")

Questions

draft-wing-avt-dtls-srtp-key-transport-02

Dan Wing, dwing@cisco.com
Backup Slides
Point to Multipoint using RFC3550 Mixer Model

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