SRTP Keying in the SIP path vs. the Media path

Lakshminath Dondeti

ldondeti@qualcomm.com

Thanks to:

Colin Perkins, Cullen Jennings, Steffen Fries, Dan Wing, Dragan Ignjatic,
Francois Audet, David McGrew, Flemming Andreasen, Jon Peterson, et. al.

Issues in SRTP/SRTCP KM

- SRTP/SRTCP crypto context
  - Keys, Salt, Lifetime, MKI and it Length for unicast or group KM
- Extent of involvement of Parties to key management
  - Distribution based model
    - One side sends keys and policy (facilitates group keying)
  - Contributory or negotiation-based model
    - Both sides negotiate policy and/or contribute entropy to key derivation
- Issues in transport selection
  - Forking, Retargeting, Forwarding
  - Early Media and Clipping
  - Latency
    - Due to transport path or due to number of messages
  - Port Control

SIP-path KM

- SDP transport of keys
  - Requires end-to-end security encapsulation
- SDP transport of key management messages
  - Authentication Key Management protocol carried in SDP
- Typically finishes within a round-trip
  - 1 RT key management protocols use Timestamps for anti-replay
    - Are additional messages ok? If so, we can do away with timestamps.
- Carried in SDP lines
  - Downgrade attacks are a concern:
    - From one mechanism to another or from SAVP to AVP
- It appears that SIP transport of KM messages cannot simultaneously address forking and clipping
- Latency: SIP answers may reach the offerer after media arrives

Media-path KM (1/3)

- Media path transport is faster: e2e communication
- Media path KM is started by the answerer
  - It takes 2 or so RTs from there for the KM protocol to finish
  - We need to be sure about the latency in this case being lower
- Senders wait until the KM finishes before sending media
  - If in-order delivery is assumed, there is no clipping
- Various options to sending KM messages via Media Path
  - UDP, RTP, and RTCP
  - Port control is an issue

Media-path KM (2/3)

- UDP: Dedicated port and needs binding to SRTP sessions
  - Port control issues; but, a one-off issue (not per session)
  - Seems like a viable candidate!
- SRTP/SRTCP: Re-use RTP/RTCP port or in-band keying
  - Re-using ports: need to be able to demultiplex
    - Possible issues with middleboxes that check for RTP packet format
      - Same issues as with ICE and not seen as a problem in future
  - In-band keying: packet expansion
    - More of an issue with RTP than RTCP; more on that latter

Media path KM (3/3)

- RTP in-band: allusions to some heads exploding
  - 3550 says header extension is for limited experimental use
  - Hard to optimize if RTP payloads are variable in size (consider rekeying also)
- Re-use RTP port: de-multiplexing and middleboxes are issues
  - Is this ok when RTP is send-only?
  - A possible candidate!
- RTCP in-band: no explosions, heads or otherwise, predicted
  - Architecturally, a logical place to send KM traffic
  - Variable size RTCP packets are not an issue
  - Issues:
    - RTCP implementation and deployment issues are a concern
    - RTCP rate control is an issue (consider rekeying also)
    - Port control may also be an issue
  - A good candidate, if some changes are anticipated on RTCP deployment!

Discussion

- Consensus calls
  - Is it worth fixing SIP-path transport?
    - Is clipping an issue?
      - Is it worth adding a third message to SIP-path transport (too much latency?)?
  - Is UDP a candidate?
  - Shall we re-use RTP port to send KM messages?
  - Is RTCP in-band keying the best option here?

- Questions, comments, opinions …