What I want to talk about …

- First talk about what this is (and not pros / cons)
- Then talk about if this is the right approach
Problem

- Some things we don’t want the middle to see (like the media content)
- Some things we want the MDD to be able to change
- Any fields the MDD changes need to be preserved somehow so the receiver can authenticate the packet E2E
The Double Solution

• Double uses normal SRTP twice – once end to end (E2E) and once between clients and MDD (HBH).

• For any RTP header field that the MDD changes, the MDD includes the original value in an RTP header extension so the receiver can authenticate the original value.

• Uses all our existing SRTP security.

• From SRTP point of view, just looks like new transform that is defined in terms of two other SRTP transforms.

• Can be modular part of existing system.
One usage scenario

- Endpoint joining a conference call sets up DTLS-SRTP session via MDD to some participant trusted with the E2E keys for call
- Normal EKT is used to provide a group key that is used for the conference
- The HBH half of the group key is given to the MDD
HBH: SRTP or not SRTP?

- SRTP requires the RTP header to be revealed to network
  - Allows diagnostic and audio quality debugging tools to work without revealing contents
  - Needed for some firewall traversal schemes

- SRTP it typically lowest bandwidth way of encrypting RTP

- Even if SRTP is not desirable, we have many ways of encrypting RTP inside another protocol other than SRTP
  - Running over IPSEC to middle box
  - Running over DTLS to middle box (very common in iOS)
  - Running over a DTLS or TLS protected TURN or HTTP Connect

- This approach supports both
  - In first case: AEAD_AES_128_GCM____AEAD_AES_128_GCM
  - In second case: AEAD_AES_128_GCM____NULL_NULL
Pro’s / Con’s

• We need to decide details of how to encode changed values
  TLV of changes vs full copy vs …. < bike shed later >

  • Very simple to specify and implement because it’s basically just calling something we already specified and implemented twice

  • Has nearly identical security properties to what we already spent years debating and approving
draft-mcgrew-srtp-aes-gcm-00 published Oct 2008

  • Leaves defining things that are useful for normal “single” encryption to the responsible WG but can use them

  • Modular and fits into existing SRTP extension mechanisms