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.
Handling things the MDD changes

• The MDD can change the Payload Type, RTP Sequence Number, or both
  – Much debate went into figuring out that is all we need (along with extensions).

• Draft defines three new RTP Header Extensions (via OHB) corresponding to above that MDD inserts to carry the changed information

• X bit derived from if there was header extensions before the OHB (Note mistake in draft of x bit)
Pro’s / Con’s

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

• Has nearly identical security properties to what we already spent years debating and approving
  – draft-mcgrew-srtp-aes-gcm-00 published Oct 2008 took 8 years to RFC

• 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
Double Packet Processing

1. Create an RTP packet
2. Encrypt with E2E key
3. Encrypt with HBH key add EKT Field
4. Decrypt with HBH key for A
5. Add OHB and encrypt with HBH key for B
6. Decrypt using HBH Key and replace OHB
7. Decrypt using E2E Key
Issue: Transform Algorithms

- DOUBLE_AEAD_AES_128_GCM_AEAD_AES_128_GCM
- DOUBLE_AEAD_AES_256_GCM_AEAD_AES_256_GCM
- DOUBLE_AEAD_AES_128_GCM_NULL_NULL
- DOUBLE_AEAD_AES_256_GCM_NULL_NULL

- Open Issue: Do We need the NULL crypto version of HBH?