Multi-Party Conferences with end-to-end Media Privacy

IETF 91 Hawaii

AVT Core Working Group

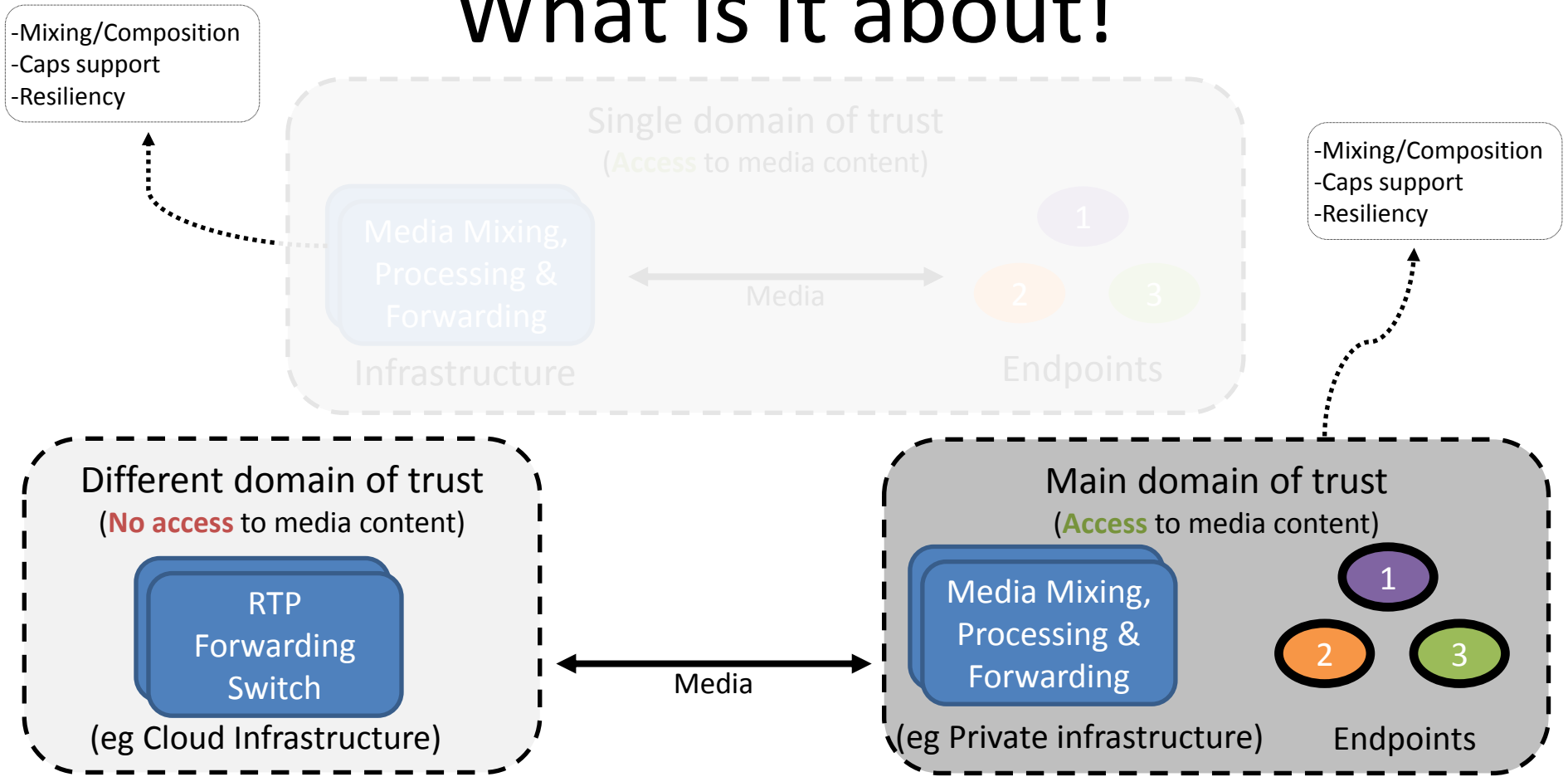
draft-jones-avtcore-private-media-reqts-00

Nermeen Ismail – Cisco Systems *John Mattsson – Ericsson Research*

Where are we?

- Two requirements and use cases drafts were presented in Toronto with lots of synergy
  - Draft-ismail-avtcore-sec-media-req-00
  - Draft-mattsson-avtcore-cloud-conferencing-use-case-00
- Drafts merged together
  - draft-jones-avtcore-private-media-reqts-00
- Paul Jones is now the prime editor

What is it about!



Media conferencing server can perform its functions without accessing or modifying secure media content

Changes since Toronto

- Single merged draft
- Better articulation of
  - What is meant by media trust in this context
  - Which components are assumed to always be in the trusted media domain
- Clarified the requirement to modify RTP headers assumes current SDP O/A model
  - Systems not reliant on SDP O/A “might” be designed
  - Must however provide a solution for clients using current O/A

Changes since Toronto

- Clarified the need for end-to-end crypto operations
  - Protect RTP payload confidentiality and integrity as it passes through non-trusted media domains
- Clarified the need for hop-by-hop crypto operations
  - Allow media components in non-trusted domain to provide per packet integrity, replay attack detection and possibility for changing RTP header fields for RTP packets
- Text on SRTCP operations using hop by hop crypto operations
- Text on the need to encrypt some RTP extension headers using hop-by-hop crypto operations (VAD is the example)
- Added a goal for solution compatibility with WebRTC security architecture
- Added requirement around optional re-keying upon changes in conference participating

Questions

- Do we to support a single RTP topology or many? If a single topology, then which?
- Clearly we need end-to-end MAC and hop-by-hop MAC, How do we include the second MAC field?
- Do we see the need to protect (encrypt, integrity) RTP extensions e2e? If so which?
- Should we put requirements on the SRTP master keys e.g. forbid group keys?
- How should the media processing steps and order look like?