Private Media Requirements in Privacy Enhanced RTP Conferencing

(draft-jones-perc-private-media-reqts-00)

IETF 93 / July 2015

Paul E. Jones

Cisco

Draft Status

- This is a revision of draft-jones-avtcore-private-media-reqts-01 presented at the last meeting
- Renamed -00 for the newly formed perc WG

What Changed

- Attempt at addressing comments made during the last meeting
- “Switching Conference Server” was renamed “Media Distribution Device” to align with charter text
- General improvements to the language of the draft
- General editorial clean-up
- Simplified the trust model (presented at the last meeting, but appearing for the first time in this draft)
- Modified some requirements (notable: PM-06, PM-09)
- Added a new requirement PM-13

PM-06 (revised)

- OLD
  - The SRTP cryptographic context, which is identified in part by an SSRC, contains transform-independent parameters used by the sending endpoint, including the RTP packet sequence number and rollover counter (ROC), required for packet decryption and authentication that, along with the value of the SSRC, MUST be protected end-to-end.
- NEW
  - A cryptographic context suitable for enabling end-to-end authenticated encryption MUST be defined.

PM-09 (revised)

- OLD
  - It MUST be possible for the switching conference server to determine if a received media packet was transmitted by a conference participant in possession of the end-to-end media encryption keys and hop-by-hop authentication keys.
- NEW
  - It MUST be possible for the switching media distribution device to determine if a received media packet was transmitted by an endpoint in possession of a valid hop-by- hop key for that conference.

PM-13 (new)

- RATIONALE
  - There were no explicit requirements for RTCP
- TEXT
  - It MUST be possible for a media distribution device or an endpoint to authenticate a received RTCP packet.