



Treatment of RTCP in PERC

Paul E. Jones
Office of the CTO, Collaboration Technology Group
January 28, 2016

RTCP Usage at the MDD

MDDs do need access to a lot of SRTCP information

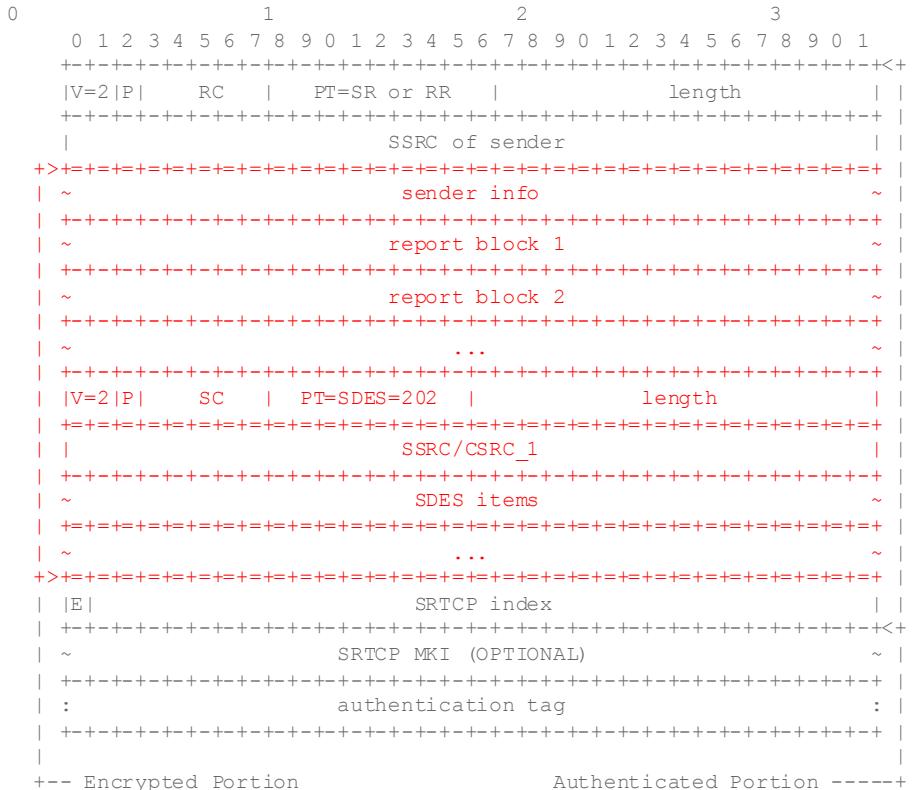
- MDDs may terminate/originate RTCP reports
- MDDs may aggregate RTCP reports from multiple participants
- Etc

Conclusion: Encrypting entire RTCP packets E2E cannot be a goal.
Encrypting hop-by-hop does allow the MDD to act on RTCP as needed.

SRTCP - E2E encryption of selected parts?

- Encrypting selected parts of an RTCP packets that an MMD does not need access to
 - Requires new procedures/changes to existing SRTP
 - Complexity and implementation risk likely delays completion the more important objective of enabling E2E media confidentiality

Conclusion: need compelling reason for E2E encryption of select subsets of RTCP info



Proposed way forward

- Perform only HBH Authentication Encryption in PERC
 - Access to the RTCP plaintext enables desired MDD operation
- Recommend that confidential info not be put into RTCP packets
 - Follow section 5 of RFC 7022 for generation of CNAME values
- If no confidential information appears in RTCP packets:
 - Access to plaintext does not compromise private user information
- If MDD is compromised, RTCP plaintext does not make attack risk any worse
 - Attacker can degrade service by discarding RTP packets regardless

