PERC ~~Design Team Meeting~~ Virtual Interim!

...

28 January 2016

WG Roadmap

Signaling
Key management
SRTP/SRTCP transforms ← you are here

Today:

- Quick recap on RTP
- Similar discussion for SRTCP

PERC is creating an entity with intermediate privilege

Normal SRTP/SRTCP divides the world into two classes:

- In the session: Can encrypt / decrypt payload, MAC/verify headers + payload
- Not in the session: Can observe header fields, encrypted payload

PERC is about creating an entity **intermediate** between these two

- Not in the session, but gets some capabilities that things in the session have
- MDD = Network Attacker + (minimum privilege to do conferencing)

For RTP...

- MDD MAY modify only PT and SEQ in header
- MDD MUST send original values
- For extension field:
  - MDD MUST NOT remove extensions
  - MDD MAY change extension value (but still send original)
  - “End to End Confidentiality Conclusion - IS DESIRABLE and NICE TO HAVE”

Questions for RTCP

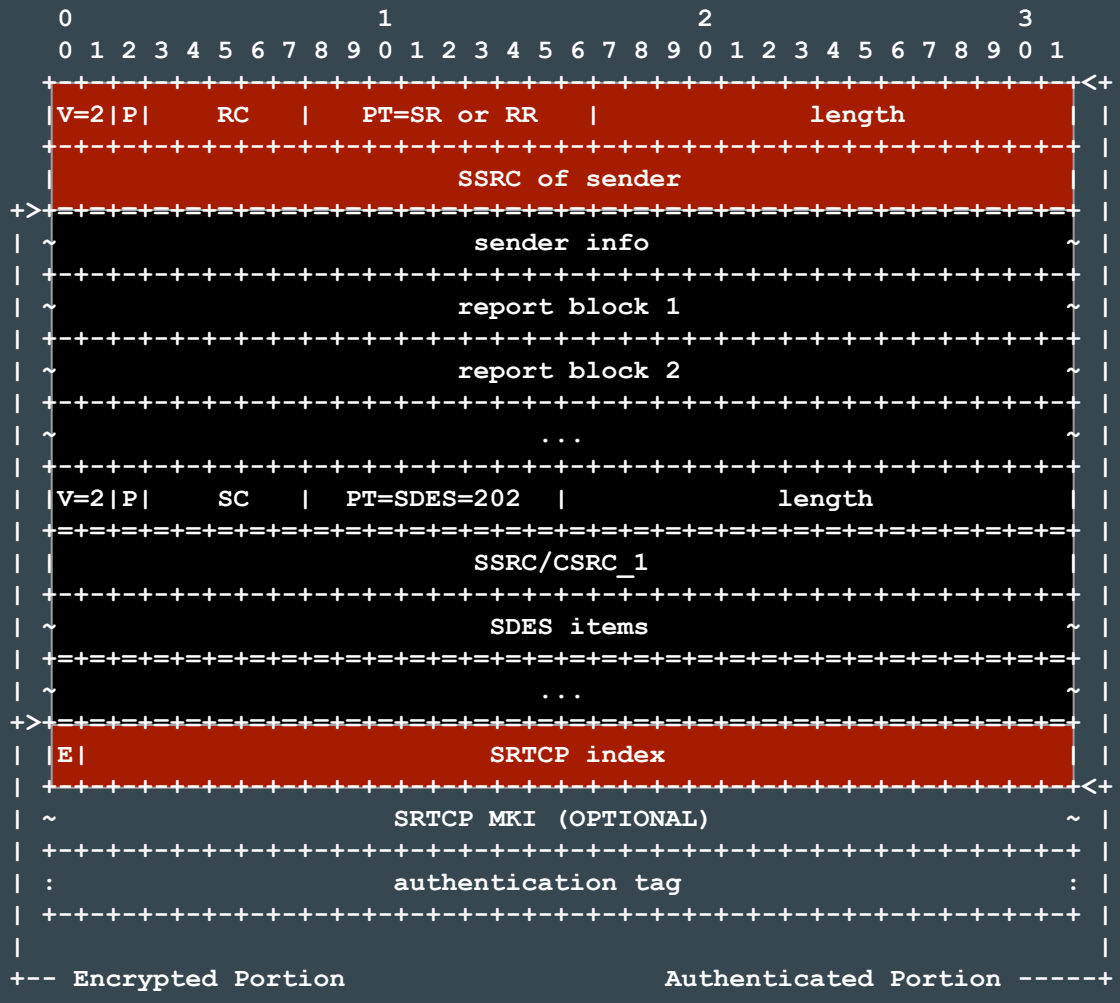
- What capabilities does the MDD need with regard to RTCP?
- Which fields does the MDD need to read?
- Which fields does the MDD need to modify?

For example: To allow MDD to do RTCP report aggregation...

[[over to Paul…]]

Authenticated

Authenticated and Encrypted



Major surgery or nothing

Multiple packets within the same security context

Only first packet's header is visible

Enabling the MDD to operate on inner packets / report blocks would involve pretty major surgery

If the MDD can't operate on inner packets, then it can't really do anything useful (mainly just change the SSRC, which we already said was immutable)

Three possible outcomes

1. MDD has no access to SRTCP (i.e., it's the same as a network attacker)
2. MDD has full access to SRTCP (i.e., it has the key)
3. Major surgery

Might be able to negotiate among these at the session / key management layer?