PERC Requirements

Paul E. Jones

IETF 94 • Yokohama

November 2015

Agenda

- Current draft text in markdown
- Proposed new requirements from John Mattsson

Requirements in Markdown

- https://github.com/paulej/perc-requirements
- It's simpler/better/cleaner to renumber the requirements 1, 2, 3… rather than PM-01, PM-02, …
  - So look to see PM- removed in subsequent revisions

Proposed New Requirements (Set 1A)

- A. The e2e replay protection MUST be provided for the whole duration of the conference
- B. The solution SHALL make it possible for a receiving endpoint to detect if the MDD delays packets for significantly longer than the network delay
- C. Endpoint joining the conference MUST authenticate the MDD

Proposed New Requirements (Set 1B)

- D. The e2e layer SHALL NOT be dependent on the hbh layer
  - Shall we use the word "layer"?
- E. It shall in the future be possible to use e.g. hbh DTLS for increased confidentiality and privacy
- F. The end-to-end keying material shall be stored securely in the endpoint and usage restricted so that it is infeasible to be extracted or use the key for anything else other than EKT

Proposed New Requirement G

- G. It SHALL be infeasible for the MDD to spoof the identity of a packet sender, including making packets from two different sending endpoints look like they originated from a single sending endpoint
  - John clarified that by "identity" he meant "the unique e2e identity, the last design meeting decided the unique e2e identity should be SSRC (but SSRC is not a good term to use as it is also a RTP field that will be changed by some MDDs)."
  - If we accept, what do we do for the term “identity” here? Just explain that on the requirement line?

Proposed New Requirement H

- H. The MDD MUST authenticate and authorize the endpoints joining the conference, ensuring that the endpoint has been invited to the conference
  - People did not seem favorable to adding this one. Shall we abandon it?

Proposed New Requirement J

- J. The service provider shall be able to enforce end-to-end security using a specific key
  - This caused some confusion, so John offered this alternative wording: “**The solution SHALL enforce end-end security using a specific key**”

Proposed New Requirement K

- K. It MUST be possible for the KMF to an function within a participating endpoint

Proposed New Requirement M

- M. The requirement should be expanded to make clear that parties that are not trusted must also not be able to use the end-to-end keying material in any other way than expected.
  - The text in PM-04 already says end-to-end keys shall not be generated or accessible by anything that is not trusted. So, do we really need this?