The Impact of Transport Header Confidentiality on Network Operation and Evolution of the Internet

draft-ietf-tsvwg-transport-encrypt-07

Gorry Fairhurst – University of Aberdeen

Colin Perkins – University of Glasgow

Feedback Received on Mailing List (1/2)

- Comments from Thomas Fossati:
  - Suggestions to clarify the text, primarily on the introductory sections
  - Suggestions for how to address the issues raised, e.g., using machine learning
    - Valuable ideas and material
    - But we think it's expanding the draft too much – would prefer to focus on the problem, and leave other drafts to recommend solutions
- Comments from Ruediger Geib:
  - Suggested additional references on how network operators may use passively collected transport layer data to optimise their networks without harming (or to improve) application performance

Feedback Received on Mailing List (2/2)

- Comments from Tom Herbert:
  - On the utility of extension headers to carry measurement information
    - e.g., ConEx can be used to convey this data
    - Believes the draft “underestimates their value and overstates the disadvantage” – such mechanisms haven’t seen much deployment so hard to evaluate
    - We agree such extension headers can be used for in-line measurement
  - On whether ossification of transport headers can ever be beneficial
    - There are examples of where this helps:
      - QUIC invariants
      - Secure RTP chose to leave some headers unencrypted, to support header compression
      - Protocol designers choosing to expose information; have a stability contract with the network
    - We believe carefully considered, intentional, ossification is acceptable – it’s unintentional ossification that’s harmful

Document Status

- Two revisions since Prague IETF meeting:
  - -06: This version expands the introductory remarks, adds some discussion of OAM-related metadata to Section 6.1, and updates the conclusions to be a little more focussed
  - -07: Revises Section 2 to reduction duplication and repetition. Clarifications around flow identification in Section 3. Expands and clarifies the conclusions and security considerations. Several, primarily editorial, corrections and clarifications throughout

- Hope to have addressed the comments

Next Steps

- Some minor editorial nits remain – will revise to address in the near term

- Believe this is ready for WG last call once those are addressed