School of
Computing Science

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

draft-fairhurst-tsvwg-transport-encrypt-09

Gorry Fairhurst – University of Aberdeen

Colin Perkins – University of Glasgow

Aims and Goals

- Transport protocols beginning to use end-to-end encryption and/or integrity protection to protect transport-layer headers

- Goals of the draft:
  - To identify in-network uses of transport layer header information
  - To review implications of transport protocols that use integrity protection and encryption to protect transport protocol header
  - To discuss impact of such changes on transport protocol design and network operation
  - Since measurement and analysis of transport protocols has been important to protocol design, to consider impact on transport and application evolution

Draft Status

- Three revisions since IETF 101
    - Address comments from Al Morton, Chris Seal, Kathleen Moriarty, Spencer Dawkins, and Joe Touch
    - Improved readability of the draft and revised to provide a more neutral view of the trade-offs
    - Greatly expanded security considerations section

Neutral Point of View

- Revised to better reflect a neutral point-of-view around the impact of transport header confidentiality, and to avoid advocating a particular position
- Expand introductory remarks on ossification as result of in-network inspection of transport headers, the wire image of the protocol, and heuristic inspection of packet timing, etc.
- Added note on implications on accountability and network neutrality

Updated Security Considerations

- Discusses implications of confidentiality and integrity protection of transport headers in avoiding ossification vs. exposing information to network
  - Limits ossification
  - Limits ability to measure and characterise traffic, detect anomalies
  - Prevents data injection attacks
- Summarises issues that are elaborated upon elsewhere in the draft

Next Steps

- Received considerable feedback over the last 18 months
- Seems to be clear interest in the work

- Trying to reflect and learn some broader lessons from development of QUIC

- Please consider adoption as TSVWG working group draft – we believe the draft is in good shape, and the topic is important to consider