UNIVERSITY OF ABERDEEN

Electronics Research Group

University of Glasgow

School of Computing Science

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

draft-ietf-tsvwg-transport-encrypt-05

Gorry Fairhurst – University of Aberdeen

Colin Perkins – University of Glasgow

Overview

This document lays out a comprehensive assessment of the impact of transport (header) encryption on network users and operators.

History

- WG -00, September 27, 2018
- WG -01, October 22, 2018 (presented IETF-103)
- WG -02, November 25, 2018
  - Comments received from Kyle Rose, Spencer Dawkins and Tom Herbert.
  - The network-layer information re-organised after IETF-103.
- WG -03, November 25, 2018
  - Added a section on header compression and rewriting of sections referring to RTP transport.
  - Author editorial work and removed duplicate section.
- WG-04, February 18, 2019
  - Updated following SecDir Review (see next slide)
- WG-05, March 9, 2019
  - Editorial update and minor corrections from comment on TSVWG list.

SecDir Review of -03
“Review result: Has issues”

- o Added some text on TLS story.
- o Section 2, paragraph 8 - changed to be clearer, in particular, added "Encryption with secure key distribution prevents”.
- o Flow label description rewritten based on PS/BCP RFCs.
- o Highlighted ways FL can be used with encryption (Section 3.1.3)
- o Added text on the explicit spin-bit work in the QUIC DT.
- o Added section on endpoint logs.
- o Added more explanation of impact on operators (Section 6).
- o Added text on greasing of spin-bit to align with QUIC (Section 6.1).
- o Added text on greasing of spin-bit to align with QUIC (Section 6.3).
- o Changed to not make it seem expensive/impossible to provide other tooling (Section 6.4).
- o Made a separate section on possible impact on R&D (section 6.5) .
- o Other comments addressed (thanks).
- o Added references.
- o Didn’t add speculation about new proposals (e.g. PEARG , things form MAPRG, - you may like to look there).

Author Review of -04
“All editorial stuff”

- We may wish to bash the summary again?

Next Steps

More feedback?

Publish?