University of Glasgow

School of Computing Science

UNIVERSITY OF ABERDEEN

Electronics Research Group

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

draft-ietf-tsvwg-transport-encrypt-01

Gorry Fairhurst – University of Aberdeen

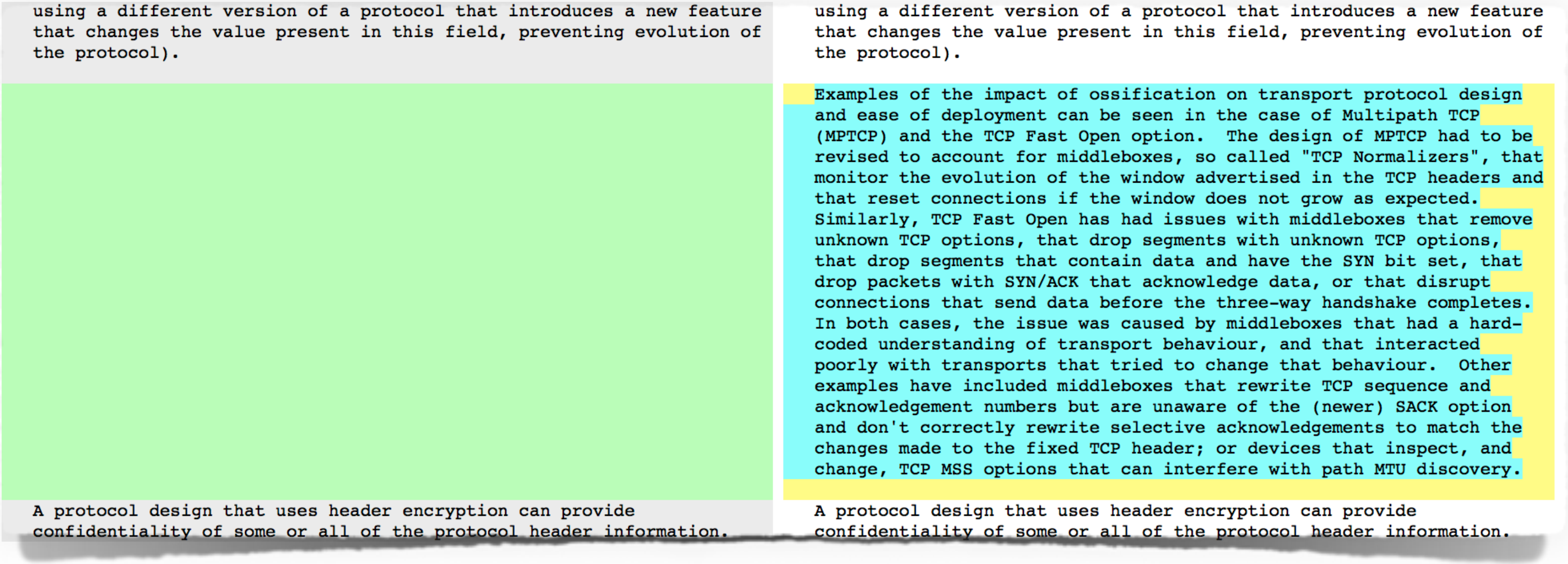
Colin Perkins – University of Glasgow

History

- The -09 individual draft was presented at IETF 102 in Montréal
- The -10 individual draft was submitted in August, addressing feedback from that meeting
- Adopted as WG item, submitted -00 with no content changes
- The -01 working group draft was submitted for this meeting

Updates since Montréal (1/2)

- Added examples of impact of ossification on transport protocols



using a different version of a protocol that introduces a new feature that changes the value present in this field, preventing evolution of the protocol).

A protocol design that uses header encryption can provide confidentiality of some or all of the protocol header information.

using a different version of a protocol that introduces a new feature that changes the value present in this field, preventing evolution of the protocol).

Examples of the impact of ossification on transport protocol design and ease of deployment can be seen in the case of Multipath TCP (MPTCP) and the TCP Fast Open option. The design of MPTCP had to be revised to account for middleboxes, so called "TCP Normalizers", that monitor the evolution of the window advertised in the TCP headers and that reset connections if the window does not grow as expected. Similarly, TCP Fast Open has had issues with middleboxes that remove unknown TCP options, that drop segments with unknown TCP options, that drop segments that contain data and have the SYN bit set, that drop packets with SYN/ACK that acknowledge data, or that disrupt connections that send data before the three-way handshake completes. In both cases, the issue was caused by middleboxes that had a hard-coded understanding of transport behaviour, and that interacted poorly with transports that tried to change that behaviour. Other examples have included middleboxes that rewrite TCP sequence and acknowledgement numbers but are unaware of the (newer) SACK option and don't correctly rewrite selective acknowledgements to match the changes made to the fixed TCP header; or devices that inspect, and change, TCP MSS options that can interfere with path MTU discovery.

A protocol design that uses header encryption can provide confidentiality of some or all of the protocol header information.

  - MP-TCP and middleboxes that track congestion window growth
  - TCP Fast Open and middleboxes that misbehave with unknown options or drop segments with data that have the SYN bit set, etc.
  - TCP SACK disruption by middleboxes that rewrite sequence numbers
  - TCP MSS rewriting middleboxes interfering with path MTU discovery

Updates since Montréal (2/2)

- Revised Introduction to better explain the purpose of the draft
- Revised discussion to better explain the choice of observation point and rationale for on-path measurements
- Reference the IAB wire image draft; update other references
- Editorial fixes throughout

Open Issues

- Review and revise conclusions – currently over-long, and doesn't make a clear point
- Discussion of metrics derived from network layer headers
  - Some has clear transport relation – ECN code points
  - Some is important operationally or for end-to-end performance, but has less clear transport interaction – IPv6 flow label; DSCP
  - Possible space for discussion of future path layer work
  - Considering whether to expand or remove this discussion
- Otherwise close to complete – looking for your input