IP Traffic Flow Security
Improving IPsec Traffic Flow Confidentiality

IETF 110 – “draft-ietf-ipsecme-iptfs-07”

Christian Hopps
LabN Consulting, LLC
Update Since IETF 109

- Transport Area Review from Joe Touch Completed
  - Suggested changes incorporated from review in -04

- Pre-WGLC WG Discussion
  - Valery
    - Request more generic identifier names
    - Fix overhead numbers and update comparison data
    - Changes published in -05
  - Tero – [pre-]WGLC review
    - Changes published in -06
Update Since IETF 109

• WGLC (3 week)
  • 1/24/2021 - 2/14/2021
  • WGLC reviews with suggested changes from:
    • Tero Kivinen
    • Sean Turner
    • Paul Wouters
    • Valery Smyslov
    • Michael Richardson

• Published -07 based on WGLC mailing list discussion
Notable Changes Through WGLC

- Normative
  - No fragmenting over multiple SAs
  - P-bit in header for PLMTUD implementations (indicates probing in progress).

- Informative
  - Editorial and organizational cleanup
  - [IP]TFS_ -> AGGFRAG_ for on-wire identifiers, as well as more generic text.
  - Expanded text on ordering packet processing on receiver
  - Expanded text on how extra padding can be used to avoid fragmentation
  - Summary of receiver actions with internal references
  - Fixed IPsec overhead for comparisons in the Appendix (same conclusions)
Moving Forward

• 3-week WGLC period completed
  • All reviews addressed, with changes incorporated

• To the IESG?
Questions and Comments