TCP Maintenance and Minor Extensions (TCPM) Monday Slot

Yoshifumi Nishida
Pasi Sarolahti
Michael Scharf

IETF 89 – London, England
March 2014

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- **By participating with the IETF, you agree to follow IETF processes.**
- **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

Agenda / Monday

- Alexander Zimmermann: Making TCP more Robust to Packet Reordering (30 min)
- Lars Eggert: PRR and NewCWV for FreeBSD (10 min)
- Mini-BoF (60 min)
  - Andrea Bittau: tcpcrypt: the case for ubiquitous transport-level encryption (30 min)
  - Technical discussion (15 min)
  - Moving forward (15 min)
- WG status, WG documents, and further presentations on Thursday

Mini-BoF

Technical Discussion

- Objective: Authentication vs. encryption vs. both?
- Existing protocols: Gap analysis?
  - TLS with TCP-AO (possibly w/ TCP-AO-NAT)?
  - "TCP Opportunistic Security (OPSEC) Option" draft-paddon-tcposp-01 (April 2009)?
- Design: Alternatives?
  - Implications of INIT? Interoperability issues?
  - MAC as option vs. payload?
- Potential compatibility issues: ECN? Data in SYN? Future options?
- Spec: Separation proto/crypto (RFC 5925/5926)?
- Implementation: Any further plans?
- Deployment: When to enable? TLS availability? LAN (latency/TSO)?
- … And: Thoughts on security?

Moving Forward

- Options for draft-bittau-tcp-crypt
  1. BoF for a new WG
     - In TSV
     - (Outside TSV)
  2. WG item in TCPM
     - "minor" TCP extension within the scope of the charter?
     - E.g., technical advisor from security area needed?
  3. WG item in MPTCP
  4. Independent submission stream
  5. No RFC at this point

- Comments?