Secure Transport for PCEP

draft-lopez-pce-pceps

IETF89 – London

Diego R. Lopez - Telefónica (diego@tid.es)
Oscar González de Dios – Telefónica (ogondio@tid.es)
Qin Wu – Huawei (sunseawq@huawei.com)
Dhruv Dhody – Huawei (dhruv.ietf@gmail.com)

The Goals

- Secure PCEP exchanges
  - Peer authentication and authorization
  - Data exchange integrity
  - Data exchange confidentiality
- Do not require change to current PCEP internals
- Do not preclude future extensions
- Allow emerging applications

The Changes

- Focus the document on TLS
  - TCP security options out of scope and discussed in the section on security considerations
  - TLS and TCP-AO deal with orthogonal problem spaces
    - TLS: E2E security with dynamic peer authentication and authorization
    - TCP-AO: Essentially, protection from DoS attacks
- Improve references to
  - Discovery (new draft on IGP extensions for security)
  - TCP security options (KARP drafts on key management)
- Provide a detailed rationale for requesting an additional port
  - We need a special message (a-la-STARTTLS)
  - Or a separate port

The (still) Open Issues

- Close the discussion on the message/port issue
  - WG consensus on this
  - Possible reluctance by Transport Area and/or IANA
- Analyze DANE applicability
  - Connecting it with DNS discovery
- Align with discovery mechanisms
  - As the I-Ds on them evolve
- Consider the application of KARP I-D on fingerprint update
  - As an additional choice for establishing trust links
  - In addition to PKI and direct configuration

- WG adoption