Secure Transport for PCEP
draft-lopez-pce-pceps

IETF88 – Vancouver

Diego R. Lopez - Telefónica (diego@tid.es)
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
TLS plus TCP-AO

• TLS
  – Transport-layer security on top of TCP
  – Common practice in several application environments
  – Unobtrusive
  – Several methods for peer identification
    • PKIX certificates being by far the most employed
  – Authentication attributes derived from peer identity token(s)
    • Flexible authorization based on attributes
  – Integrity and confidentiality

• TCP-AO
  – Authenticated source for TCP packets
  – Relies on external key management
  – Integrity of the transport stream
Why TLS plus TCP-AO

• Unobtrusive
• Satisfy security requirements
• TLS is a well-known and established practice
  – Above all, richer identity management
    • Dynamic decision on peer identity and rights
    • Attribute-based access control
    • Attribute-based policy
  – Supporting richer models
    • Dynamic discovery
    • Flexible hierarchies
    • Inter-domain agreements
    • Future SDN-based approaches
• TCP-AO is complementary to TLS
  – Enhanced security of the transport stream
  – Able to rely on TLS for key management
PKI (Generally Speaking)

• Does not imply
  – A single, global root of trust run by an external party
    • Several are possible (and desirable in many cases)
    • As local as is required
  – Additional complexity on key management or cumbersome administrative procedures
    • Beyond whatever PSK mechanism implies

• And brings
  – Dynamic trust links
  – Application of identity-based policies
PCEPS

- Reserved port for PCEP operation on TLS
  - No inline TLS start negotiation
  - Port number allocation to be requested to IANA

- TCP-AO usage is OPTIONAL
  - Recommended for long-lived connections
  - Possible Master Key Tuple derivation from TLS key material

- TLS 1.2 with
  - REQUIRED mutual peer authentication
  - REQUIRED integrity
  - RECOMMENDED confidentiality
  - OPTIONAL compression

- Peer authentication by means of certificates
Peer AuthN / AuthZ

• Certificate validation by
  – PKIX trust models
    • RECOMMENDED check of FQDN and/or IP address
  – Trusted certificates by means of fingerprints
    • Almost PSK
• OPTIONAL application of additional checks on attributes transported in the certificate
  – FQDN(s) and IP address(es)
  – Issuer and Subject
  – Alternate names
  – Certificate policies
  – Key usage
  – . . .
Coming Steps

• PCEPS port
• DANE applicability
• Connection with discovery
  – IGP advertisement
  – DNS-based
• Linking TCP-AO and TLS
  – Delineate conditions for requiring both
  – MKT management