IGP extension for PCEP security capability support in the PCE discovery

draft-ietf-lsr-pce-discovery-security-support-01

Zitao Wang
Qin Wu
Dhruv Dhody
Daniel King
Diego Lopez
IETF 105
Montreal Canada
July 20~26, 2019

Status Update

- Two week adoption call on draft-wu-lsr-pce-discovery-security-support-00 started in November 13 and concluded in November 26
  - Agree to update RFC5088 and RFC5089 to allow advertisement of KEY-ID or Key Chain Name Sub-TLV to support TCP AO security capability.
  - Create registry for PCED Sub-TLV Type indicator
  - Allow KEY ID and Key Chain Name Sub-TLV present in the PCED sub-TLV carried within the IS-IS Router Information Capability TLV
  - Remove duplicate text related to RFC5088 and RFC5089

- Draft-wu-lsr-pce-discovery-security-support-01 address the above comments and adopted as LSR WG draft in December 4,2018

Discussion: PCE Position (1)

- This draft was adopted by LSR WG without PCE WG endorsement
  - Although it was discussed in PCE WG in the past
- PCE WG should take position on:
  - Removes the restriction specified in RFC 5088/5089 of not allowing further PCE related advertisements in Router Capability TLV/Router Information LSA.
    - Con:
      - Advertise information not directly relevant to the operation of the IGP impact performance of IGP function
    - Pro:
      - The security communication consideration between PCE and PCC is important
      - piggyback action can simplify the operation of network. Or else, the network should operate different protocols to accomplish such task.

Discussion: PCE Position (2)

- Write an RFC5088/89bis document or separate extension document?
  - Update RFC5089/5089 in draft-ietf-lsr-discovery-security-support document
  - Make RFC5088/89bis document to incorporate draft-ietf-lsr-discovery-security-support

Next Step

- Comments and feedback, input?
- Keep on progress this draft in LSR or move to PCE WG?

Recap

- Security protection for routing protocol such as PCEP, BGP is important
  - TCP-MD5(RFC2385) Provides integrity, but doesn't protect against IP header stuff. Deprecated due to being weak.
  - TLS (RFC5246). Well deployed
  - IPSec. Largly just works, but
    - Not work well with NAT boxes
    - Slow session establishment, Bootstrapping issue
  - TCP AO (RFC5925) address many deficiency of TCP-MD5, and add key agility, but lack widely deployment.
- Before connecting to a PCE server with TLS support, TCP AO, TCP MD5, PCC needs to know which PCE server supports TLS, TCP AO,etc.
- Without using discovery, it leads to unexpected failure or additional message exchange is needed to indicate error to PCC using PCErr message.
- Proposes new capability flag bits for PCE-CAP-FLAGS sub-TLV that can be announced as attributes in the IGP advertisement to distribute PCEP security support information.
  - E.g., PCE with TLS support
  - PCE with TCP-MD5 support
  - PCE with TCP-AO support