IGP extension for PCEP security capability support in the PCE discovery

draft-wu-lsr-discovery-security-support-00

Zitao Wang
Qin Wu
Dhruv Dhody
Daniel King
Diego Lopez

IETF 103
Bangkok, Tailand
Oct 12, 2018

Recap

- Security protection for routing protocol such as PCEP, BGP
  - TCP-MD5(RFC2385) Provides integrity, but doesn’t protect against IP header stuff. Deprecated due to being weak.
  - TLS (RFC5246). Well deployed
  - IPSec. Largely 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.
    - This will be changed soon when more and more vendors implement TCP AO(e.g.,TCP AO implementation hackathon work in IETF 103).

Motivation

- RFC8253(PCEPS) describes using TLS to enhance PCEP security. This requires that both PCC and PCE server should support TLS

- 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.

- The current PCE discovery protocol define in [RFC5088] and [RFC5089] doesn’t provide such capability

- Without using discovery, it leads to unexpected failure or additional message exchange is needed to indicate error to PCC using PCErr message.

Solution

- PCE-CAP-FLAGS sub- TLV is defined in [RFC5088] and [RFC5089] to advertise PCE capability.

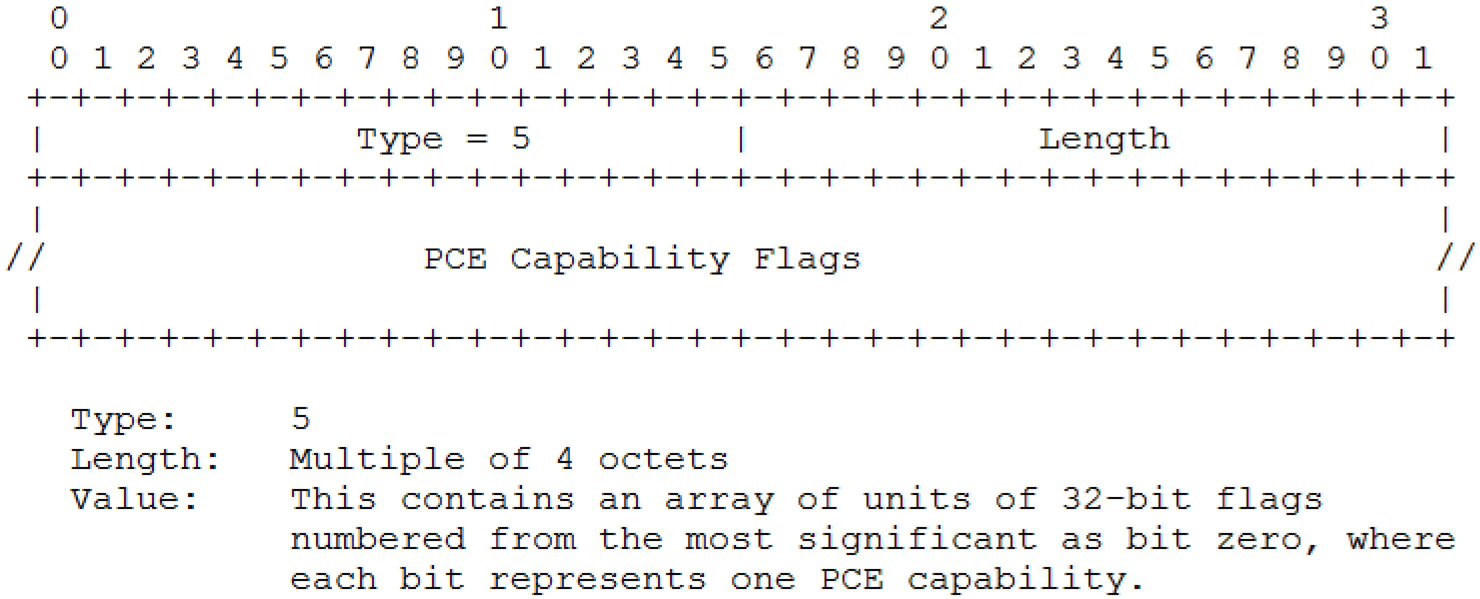
- Proposes new capability flag bits for PCE-CAP-FLAGS sub-TLV that can be announced as attributes in the IGP advertisement

  to distribute PCEP security support information.

  - E.g., PCE with TLS support
  - PCE with TCP-MD5 support
  - PCE with TCP-AO support

New flag bits in PCE-CAP-FLAGS sub- TLV

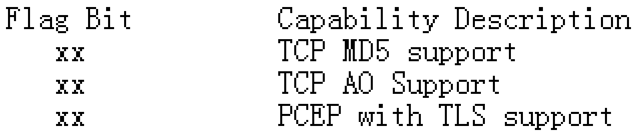
- PCEP-CAP-FLAGS Sub-TLV format



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Type = 5           |              Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                                |
//                  PCE Capability Flags                        //
|                                                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

  Type:      5
  Length:    Multiple of 4 octets
  Value:     This contains an array of units of 32-bit flags
             numbered from the most significant as bit zero, where
             each bit represents one PCE capability.
```

In the PCE capability Flags field, we add three new flag bits as follows:



Flag Bit	Capability Description
xx	TCP MD5 support
xx	TCP AO Support
xx	PCEP with TLS support

Open Issue: Include Key-ID

- Add key-id for TCP-AO or TLS usage
  - the key-chain name from RFC 8177
  - Add details security parameter raises security concern
    - E.g.,include the actual keys in IGPs
    - Having actual key in BGP
- Proposal:
  - Only add key-id for TCP-AO or TLS usage.

Next Step

- Adoption?

With Discovery

- * With discovery - PCE requiring TLS
  - PCC uses discovery to know it needs to use TLS to connect to the desired PCE
  - PCC initiates TCP connection and TLS handshake
  - PCEP exchange within TLS context
- * With discovery – PCE not requiring TLS
  - PCC uses discovery to know it needs not to use TLS to connect to the desired PCE
  - PCC initiates TCP connection
  - PCEP exchange over TCP

Without Discovery

- * Without discovery - PCE requiring TLS
  - 1.- PCC initiates TCP connection and TLS handshake
  - 2.- PCEP exchange within TLS context
- ---
  - 1.- PCC initiates TCP connection and attempts a PCEP OPEN message
  - 2.- PCE rejects the message with a PCErr message (Error-Type=1, Error-value=3, TLV identifying the need for TLS)
  - (optionally)
  - 3.- PCC initiates TCP connection and TLS handshake
  - 4.- PCEP exchange within TLS context

- * Without discovery - PCE not requiring TLS
  - 1.- PCC initiates TCP connection
  - 2.- PCEP exchange over TCP
- ---
  - 1.- PCC initiates TCP connection and TLS handshake
  - 2.- No TLS context established with PCE or error message received
  - (optionally)
  - 3.- PCC initiates TCP connection
  - 4.- PCEP exchange over TCP