     IGP extension for PCEP security capability support in the PCE discovery
            draft-wu-lsr-pce-discovery-security-support-00

Abstract

   When a Path Computation Element (PCE) is a Label Switching Router
   (LSR) participating in the Interior Gateway Protocol (IGP), or even a
   server participating in IGP, its presence and path computation
   capabilities can be advertised using IGP flooding. The IGP
   extensions for PCE discovery (RFC 5088 and RFC 5089) define a method
   to advertise path computation capabilities using IGP flooding for
   OSPF and IS-IS respectively. However these specifications lack a
   method to advertise PCEP security (e.g., Transport Layer
   Security(TLS),TCP Authentication Option (TCP-AO)) support capability.

   This document proposes new capability flag bits for PCE-CAP-FLAGS
   sub-TLV that can be announced as attribute in the IGP advertisement
   to distribute PCEP security support information.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at https://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on February 24, 2019.

1. Introduction

   As described in [RFC5440], PCEP communication privacy is one
   importance issue, as an attacker that intercepts a Path Computation
   Element (PCE) message could obtain sensitive information related to
   computed paths and resources.

   Among the possible solutions mentioned in these documents, Transport
   Layer Security (TLS) [RFC5246] provides support for peer
   authentication, and message encryption and integrity while TCP
   Authentication Option (TCP-AO) [RFC5925] and Cryptographic Algorithms
   for TCP-AO [RFC5926] offer significantly improved security for
   applications using TCP. As specified in section 4 of [RFC8253], in
   order for a Path Computation Client(PCC) to begin a connection with a
   PCE server using TLS or TCP-AO, PCC SHOULD know whether PCE server
   supports TLS or TCP-AO as a secure transport.

   [RFC5088] and [RFC5089] define a method to advertise path computation
   capabilities using IGP flooding for OSPF and IS-IS respectively.
   However [RFC5088] and [RFC5089] lacks a method to advertise PCEP
   security (e.g., TLS) support capability.

   This document proposes new capability flag bits for PCE-CAP-FLAGS
   sub-TLV that can be announced as attributes in the IGP advertisement
   (defined in [RFC5088] and [RFC5089]) to distribute PCEP security
   support information.

2. Conventions used in this document

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC2119 [RFC2119].

3. IGP extension for PCEP security capability support

   The PCE-CAP-FLAGS sub-TLV is defined in section 4.5 of [RFC5088] and
   [RFC5089] as an optional sub-TLV used to advertise PCE capabilities.
   In this section, we extend the PCE-CAP-FLAGS sub-TLV to include the
   capability and indications that are described for PCEP security
   (e.g., TLS) support in the current document.

   In the PCE-CAP-FLAGS sub-TLV defined in [RFC5088] and [RFC5089], nine
   capability flags defined in [RFC5088] (as per [RFC4657]) and two
   capability flags defined [RFC5557], [RFC6006] are included and
   follows the following format:

      o TYPE: 5
      o LENGTH: Multiple of 4
      o VALUE: This contains an array of units of 32 bit flags with
         the most significant bit as 0. Each bit represents one PCE
         capability.

   and the processing rule of these flag bits are defined in [RFC5088]
   and [RFC5089]. In this document, we define two new capability flag
   bits that indicate TCP Authentication Option (TCP-AO) support, PCEP
   over TLS support respectively as follows:

         Bit   Capability Description
         xx   TCP AO Support
         xx   PCEP over TLS support

3.1. Use of PCEP security capability support for PCE discovery

   TCP-AO, PCEP over TLS support flag bits are advertised using IGP
   flooding.

   o PCE supports TCP-AO: IGP advertisement SHOULD include TCP-AO
      support flag bit.

   o PCE supports TLS: IGP advertisement SHOULD include PCEP over TLS
      support flag bit.

   If PCE supports multiple security mechanisms, it SHOULD include all
   corresponding flag bits in IGP advertisement.

   If the client is looking for connecting with PCE server with TCP-AO
   support, the client MUST check if TCP-AO support flag bit in the PCE-
   CAP-FLAGS sub-TLV is set. If not, the client SHOULD NOT consider
   this PCE. If the client is looking for connecting with PCE server
   using TLS, the client MUST check if PCEP over TLS support flag bit in

the PCE-CAP-FLAGS sub-TLV is set. If not, the client SHOULD NOT
consider this PCE.

4. Backward Compatibility Consideration

An LSR that does not support the new IGP PCE capability bits
specified in this document silently ignores those bits.

IGP extensions defined in this document do not introduce any new
interoperability issues.

5. Management Considerations

A configuration option may be provided for advertising and
withdrawing PCE security capability via IGP.

6. Security Considerations

This document raises no new security issues beyond those described in
[RFC5088] and [RFC5089].

7. IANA Considerations

IANA is requested to allocate a new bit in "PCE Security Capability
Flags" registry for PCEP Security support capability.

```
     Bit             Meaning                 Reference
     xx              TCP-AO Support          [This.I.D]
     xx              PCEP over TLS support   [This.I.D]
```

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", March 1997.

[RFC5088] Le Roux, JL., "OSPF Protocol Extensions for Path
           Computation Element (PCE) Discovery", RFC 5088, January
           2008.

[RFC5089] Le Roux, JL., "IS-IS Protocol Extensions for Path
           Computation Element (PCE) Discovery", RFC 5089, January
           2008.

[RFC5925] Touch , J., "The TCP Authentication Option", RFC 5925,
           June 2010.

   [RFC5926] Gregory Lebovitz, G., "Cryptographic Algorithms for the
              TCP Authentication Option (TCP-AO)", RFC 5926, June 2010.

   [RFC8253] R. Lopez, D., "PCEPS: Usage of TLS to Provide a Secure
              Transport for the Path Computation Element Communication
              Protocol (PCEP)", RFC 8253, October 2017.

8.2. Informative References

   [RFC4657] Ash, J. and J. Le Roux, "Path Computation Element (PCE)
              Communication Protocol Generic Requirements", RFC 4657,
              September 2006.

   [RFC5246] Dierks, T., "The Transport Layer Security (TLS) Protocol
              Version 1.2", RFC 5246, August 2008.

   [RFC5440] Le Roux, JL., "Path Computation Element (PCE)
              Communication Protocol (PCEP)", RFC 5440, March 2009.

   [RFC5557] Lee, Y., Le Roux, JL., King, D., and E. Oki, "Path
              Computation Element Communication Protocol (PCEP)
              Requirements and Protocol Extensions in Support of Global
              Concurrent Optimization", RFC 5557, July 2009.

   [RFC6006] Zhao, Q., King, D., Verhaeghe, F., Takeda, T., Ali, Z.,
              and J. Meuric, "Extensions to the Path Computation Element
              Communication Protocol (PCEP) for Point-to-Multipoint
              Traffic Engineering Label Switched Paths", RFC 6006,
              September 2010.

Appendix A. Appendix A: No MD5 Capability Support

   To be compliant with Section 10.2 of RFC5440, this document doesn't
   consider to add capability for TCP-MD5. Therefore by default, PCEP
   Speaker in communication supports capability for TCP-MD5 (See section
   10.2,[RFC5440]). A method to advertise TCP-MD5 Capability support
   using IGP flooding is not required. If the client is looking for
   connecting with PCE server with other Security capability support
   (e.g., TLS support) than TCP-MD5, the client MUST check if flag bit
   in the PCE- CAP-FLAGS sub-TLV for specific capability is set (See
   section 3.1).

Authors' Addresses

   Diego R. Lopez
   Telefonica I+D
   Spain

   Email: diego.r.lopez@telefonica.com

   Qin Wu
   Huawei Technologies
   12 Mozhou East Road, Jiangning District
   Nanjing, Jiangsu 210012
   China

   Email: bill.wu@huawei.com

   Dhruv Dhody
   Huawei Technologies
   Divyashree Techno Park, Whitefield
   Bangalore, Karnataka 560037
   India

   Email: dhruv.ietf@gmail.com

   Michael Wang
   Huawei
   12 Mozhou East Road, Jiangning District
   Nanjing, Jiangsu 210012
   China

   Email: wangzitao@huawei.com

   Daniel King
   Old Dog Consulting
   UK

   Email: daniel@olddog.co.uk