IGP extension for PCEP security capability support in the PCE discovery
draft-wu-pce-discovery-pceps-support-01

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)) support capability.

This document proposes new capability flag bit 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 http://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 14, 2015.
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. In order for a Path Computation Client (PCC) to begin a connection with a PCE server using TLS, PCC SHOULD know whether PCE server supports TLS 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.

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:

- TYPE: 5
- LENGTH: Multiple of 4
- 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 three new capability flag bits that indicate TCP MD5 support, TCP Authentication Option (TCP-AO) support, PCEP over TLS support respectively as follows:

<table>
<thead>
<tr>
<th>Bit</th>
<th>Capability Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx</td>
<td>TCP MD5 support</td>
</tr>
<tr>
<td>xx</td>
<td>TCP AO Support</td>
</tr>
<tr>
<td>xx</td>
<td>PCEP over TLS support</td>
</tr>
</tbody>
</table>

Editor Note: TCP-MD5 is a MUST in RFC5440, do we need a capability for it?

3.1. Use of PCEP security capability support for PCE discovery

TCP MD5, TCP-AO, PCEP over TLS support flag bits are advertised using IGP flooding.
o PCE supports TCP MD5: IGP advertisement SHOULD include TCP MD5 support flag bit.

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-MD5 support, the client MUST check if TCP-MD5 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 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 MD5 support          [This.I.D]
xx   TCP-AO Support          [This.I.D]
xx   PCEP over TLS support   [This.I.D]

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses