PCE working group
Internet-Draft
Updates: 5088,5089 (if approved)
Intended status: Standards Track
Expires: June 7, 2019

D. Lopez
Telefonica I+D
Q. Wu
D. Dhody
Z. Wang
Huawei
D. King
Old Dog Consulting

December 4, 2018

IGP extension for PCEP security capability support in the PCE discovery

draft-ietf-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. In addition, this document updates RFC 5088 and RFC 5089 to allow advertisement of Key ID or Key Chain Name Sub-TLV to support TCP AO security capability.

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 June 7, 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) [RFC8446] 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 needs to 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 these specifications lack 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 to distribute PCEP security support information. In addition, this document updates RFC5088 and RFC5089 to allow advertisement of Key ID or Key Chain Name Sub-TLV to support TCP AO security capability.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. IGP extension for PCEP security capability support

[RFC5088] defines a PCE Discovery (PCED) TLV carried in an OSPF Router Information Link State Advertisement (LSA) as defined in [RFC7770] to facilitate PCE discovery using OSPF. This document defines two new capability flag bits in the OSPF PCE Capability Flags to indicate TCP Authentication Option (TCP-AO) support [RFC5925][RFC5926], PCEP over TLS support [RFC8253] respectively.

Similarly, [RFC5089] defines the PCED sub-TLV for use in PCE discovery using IS-IS. This document will use the same flag for the OSPF PCE Capability Flags sub-TLV to allow IS-IS to indicate TCP Authentication Option (TCP-AO) support, PCEP over TLS support respectively.

The IANA assignments for shared OSPF and IS-IS Security Capability Flags are documented in Section 8.1 ("OSPF PCE Capability Flag") of this document.

3.1. Use of PCEP security capability support for PCE discovery

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

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

- 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

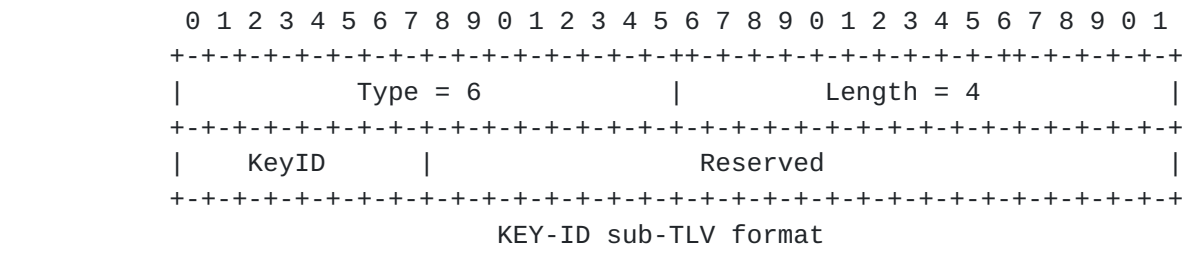
consider this PCE. Note that this can be overridden based on a local policy at the PCC.

3.2. KEY-ID Sub-TLV

The KEY-ID sub-TLV specifies a key that can be used by the PCC to identify the TCP-AO key [RFC5925].

The KEY-ID sub-TLV MAY be present in the PCED sub-TLV carried within the IS-IS Router Information Capability TLV when the capability flag bit of PCE-CAP-FLAGS sub-TLV in IS-IS is set to indicate TCP Authentication Option (TCP-AO) support. Similarly, this sub-TLV MAY be present in the PCED TLV carried within OSPF Router Information LSA when the capability flag bit of PCE-CAP-FLAGS sub-TLV in OSPF is set to indicate TCP-AO support.

The format of the KEY-ID sub-TLV is as follows:



KEY-ID sub-TLV format

Type: 6

Length: 4

KeyID: The one octed Key ID as per [RFC5925] to uniquely identify the Master Key Tuple (MKT).

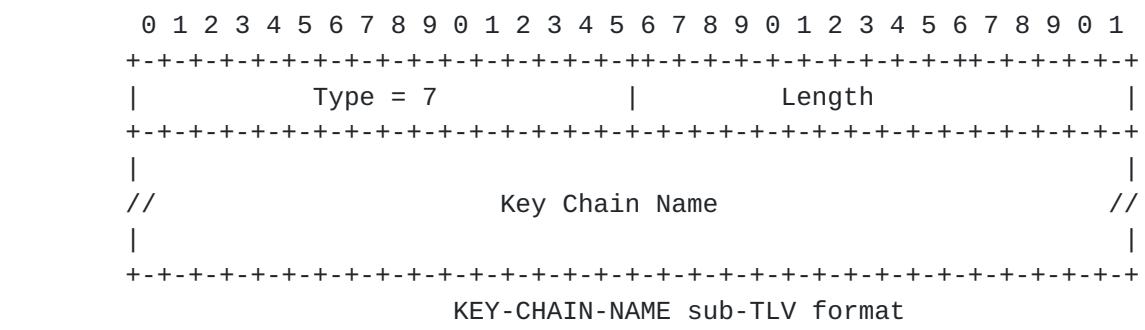
Reserved: MUST be set to zero while sending and ignored on receipt.

3.3. KEY-CHAIN-NAME Sub-TLV

The KEY-CHAIN-NAME sub-TLV specifies a keychain name that can be used by the PCC to identify the keychain [RFC8177].

The KEY-CHAIN-NAME sub-TLV MAY be present in the PCED sub-TLV carried within the IS-IS Router Information Capability TLV when the capability flag bit of PCE-CAP-FLAGS sub-TLV in IS-IS is set to indicate TCP Authentication Option (TCP-AO) support. Similarly, this sub-TLV MAY be present in the PCED TLV carried within OSPF Router Information LSA when the capability flag bit of PCE-CAP-FLAGS sub-TLV in OSPF is set to indicate TCP-AO support.

The format of the KEY-CHAIN-NAME sub-TLV is as follows:



KEY-CHAIN-NAME sub-TLV format

Type: 7

Length: Variable

Key Name: The Key Chain Name contains a string to be used to identify the key chain. It SHOULD be a string of printable ASCII characters, without a NULL terminator. The TLV MUST be zero-padded so that the TLV is 4-octet aligned.

4. Update to RFC5088 and RFC5089

Section 4 of [RFC5088] needs to be updated to allow advertisement of additional PCE information carried in the Router Information LSA. The following is proposed text for this change.

Replace the following paragraph from section 4:

"No additional sub-TLVs will be added to the PCED TLV in the future. If a future application requires the advertisement of additional PCE information in OSPF/ISIS, this will not be carried in the Router Information LSA."

with

"If a future application requires the advertisement of additional PCE information in OSPF, e.g., to facilitate key distribution and cryptographic authentication and message integrity verification, additional sub-TLVs could be added to the PCED TLV and carried in the Router Information LSA."

Section 4 of [RFC5089] needs to be updated to allow advertisement of additional PCE information carried in the Router CAPABILITY TLV. The following is proposed text for this change.

Replace the following paragraph from section 4:

"No additional sub-TLVs will be added to the PCED TLV in the future. If a future application requires the advertisement of additional PCE information in IS-IS, this will not be carried in the CAPABILITY TLV."

with

"If a future application requires the advertisement of additional PCE information in IS-IS, e.g., to facilitate key distribution and cryptographic authentication and message integrity verification, additional sub-TLVs could be added to the PCED sub-TLV and carried in the CAPABILITY TLV."

At a time of publication of [RFC5088] and [RFC5089] there were concerns about advertising non-IGP specific information in OSPF(v3) Router Information LSAs and IS-IS router capability TLV. [RFC7770] added the functionality of advertising multiple instances of the OSPF(v3) Router Information LSA and IS-IS support multiple CAPABILITY TLV [RFC7981].

5. Backward Compatibility Consideration

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

An LSR that does not support the new KEYNAME sub-TLV specified in this document silently ignores the sub-TLV.

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

6. Management Considerations

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

7. Security Considerations

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

8. IANA Considerations

8.1. OSPF PCE Capability Flag

IANA is requested to allocate new bits assignments for the OSPF Parameters "Path Computation Element (PCE) Capability Flags" registry.

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

The registry is located at: https://www.iana.org/assignments/ospfv2-parameters/ospfv2-parameters.xml#ospfv2-parameters-14.xml

8.2. PCED sub-TLV Type Indicators

The PCED sub-TLVs were defined in [RFC5088] and [RFC5089], but they did not create a registry for it. This document requests IANA to create a new top-level OSPF registry, the "PCED sub-TLV type indicators" registry. This registry should be populated with -

Value	Description	Reference
0	Reserved	[This.I.D][RFC5088]
1	PCE-ADDRESS	[This.I.D][RFC5088]
2	PATH-SCOPE	[This.I.D][RFC5088]
3	PCE-DOMAIN	[This.I.D][RFC5088]
4	NEIG-PCE-DOMAIN	[This.I.D][RFC5088]
6	KEY-ID	[This.I.D]
7	KEY-CHAIN-NAME	[This.I.D]

This registry is also used by IS-IS PCED sub-TLV.

9. Acknowledgments

The authors of this document would also like to thank Acee Lindem, Julien Meuric for the review and comments.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5088] Le Roux, JL., Ed., Vasseur, JP., Ed., Ikejiri, Y., and R. Zhang, "OSPF Protocol Extensions for Path Computation Element (PCE) Discovery", RFC 5088, DOI 10.17487/RFC5088, January 2008, <https://www.rfc-editor.org/info/rfc5088>.

[RFC5089] Le Roux, JL., Ed., Vasseur, JP., Ed., Ikejiri, Y., and R. Zhang, "IS-IS Protocol Extensions for Path Computation Element (PCE) Discovery", RFC 5089, DOI 10.17487/RFC5089, January 2008, <https://www.rfc-editor.org/info/rfc5089>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)", RFC 5926, DOI 10.17487/RFC5926, June 2010, <https://www.rfc-editor.org/info/rfc5926>.

[RFC7770] Lindem, A., Ed., Shen, N., Vasseur, JP., Aggarwal, R., and S. Shaffer, "Extensions to OSPF for Advertising Optional Router Capabilities", RFC 7770, DOI 10.17487/RFC7770, February 2016, <https://www.rfc-editor.org/info/rfc7770>.

[RFC7981] Ginsberg, L., Previdi, S., and M. Chen, "IS-IS Extensions for Advertising Router Information", RFC 7981, DOI 10.17487/RFC7981, October 2016, <https://www.rfc-editor.org/info/rfc7981>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8177] Lindem, A., Ed., Qu, Y., Yeung, D., Chen, I., and J. Zhang, "YANG Data Model for Key Chains", RFC 8177, DOI 10.17487/RFC8177, June 2017, <https://www.rfc-editor.org/info/rfc8177>.

[RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)", RFC 8253, DOI 10.17487/RFC8253, October 2017, <https://www.rfc-editor.org/info/rfc8253>.

10.2. Informative References

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

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