Network Working Group
Internet-Draft
Intended status: Informational
Expires: 3 September 2025

K. Xu
X. Wang
Z. Liu
Q. Li
J. Wu
Tsinghua University
Y. Guo
Zhongguancun Laboratory
J. Wu
Tsinghua University

2 March 2025

A profile for FC path attribute
draft-wang-idr-fc-path-attribute-00

Abstract

This document specifies a mechanism for embedding a new path attribute, known as the FC path attribute, into BGP UPDATE messages. The FC (Forwarding Commitment) is a cryptographically signed object to certify an AS's routing intent on its directly connected hops. By incorporating the FC path attribute into BGP UPDATE messages, this mechanism provides enhanced route authenticity and lays the groundwork for improved data-plane forwarding verification. This mechanism is backward compatible, which means a router that supports the attribute can interoperate with a router that doesn't, allowing partial deployment across the Internet.

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 3 September 2025.

Table of Contents

1. Introduction

This document describes the FC path attribute, a new attribute for providing path security for Border Gateway Protocol (BGP) [RFC4271] route advertisements. That is, a BGP speaker who receives a valid BGP UPDATE message with FC path attribute has the following property: every Autonomous System (AS) on the path of ASes listed in the UPDATE message with a corresponding FC has explicitly authorized the advertisement of the route from the former AS to the subsequent AS in the path. This allows verification of the AS path in the BGP UPDATE messages and data-plane forwarding.

The FC path attribute is an optional and transitive BGP path attribute. This attribute can be used by an BGP speaker supporting it to generate, propagate and validate BGP UPDATE messages containing this attribute to obtain the above assurances.

A FC path attribute consists of mainly one or multiple Forwarding Commitments (FC). The FC path attribute is intended to be used to supplement BGP origin validation [RFC6483] [RFC6811]. As the AS_PATH attribute is preserved and each Forwarding Commitment (FC) is a publicly verifiable code certifying the correctness of a three-hop pathlet, FC path attribute can provide more security than BGPsec [RFC8205] in the case of partial deployment.

The FC path attribute needs to be associated with an additional mechanism for providing the distribution of AS numbers and managing keys. The Resource Public Key Infrastructure (RPKI) [RFC8209] is one of the optiions.

2. Terminology

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. The FC Path Attribute

The FC path attribute is an optional and transitive BGP path attribute within the BGP UPDATE message. BGP speakers do not recognize the FC path attribute SHOULD still transmit this attribute to their neighbors. AS a result, there is no need to establish a new BGP capability as defined in [RFC5492].

The FC path attribute consists mainly of one or multiple Forward Commitments (FC). The FC carries the secured information regarding the intent of an AS to propagate the route between neighboring ASes, and includes the digital signature used to protect the information. The FC path attribute is independent and doesn’t affect other attributes in the BGP UPDATE message. Althouge the FC path attribute would not modify the AS_PATH path attribute, it is REQUIRED to never use the AS_SET or AS_CONFED_SET according to [RFC6472].

3.1. Forwarding Commitment

A detailed description of the Forwarding Commitment information in the FC path attribute is provided here. The specification for the Forwarding Commitment is provided in Figure 1.

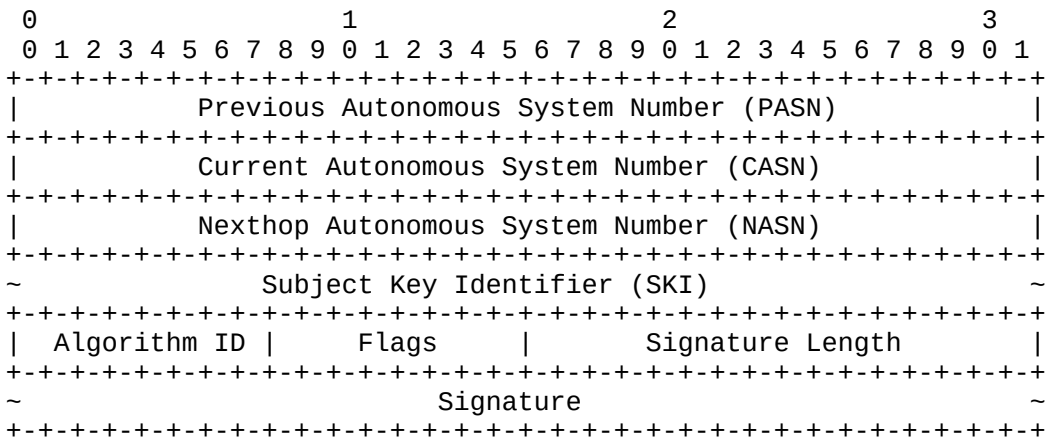

Figure 1: The structure of Forwarding Commitment

In the FC path attribute, all ASs MUST use 4-byte AS numbers in FC secments. Existing 2-byte AS numbers are converted into 4-nyte AS numbers by setting the two high-order octets of the 4-octet field to 0 [RFC6793].

FC segment includes the following parts.

Previous Autonomous System Number (PASN, 4 octets): The PASN is the AS number of the previous hop AS from whom the BGP speaker receives the BGP UPDATE message. If the current AS has no previous AS hop, it MUST be filled with 0.

Current Autonomous System Number (CASN, 4 octets): The CASN is the AS number of the BGP speaker that added this FC segment to the FC path attribute.

Nexthop Autonomous System Number (NASN, 4 octets): The NASN is the AS number of the next hop AS to whom the BGP speaker will send the BGP UPDATE message.

Subject Key Identifier (SKI, 20 octets): The SKI is a unique identifier for the public key used for signature verification. If the SKI length exceeds 20 octets, it should retrieve the leftmost 20 octets.

Algorithm ID (1 octet): The current assigned value is 1, indicating that SHA256 is used to hash the content to be signed, and ECDSA is used for signing. It follows the algorithm suite defined in [RFC8208] and its updates. Each FC segment has an Algorithm ID, so

there is no need to worry about sudden changes in its algorithm suite. The key in FC-BGP uses the BGPsec Router Key, so its generation and management follow [RFC8635].

Flags (1 octet): Several flag bits. The leftmost bit of the Flags field is the Confed_Segment flag (Flags-CS). The Flags-CS flag is set to 1 to indicate that the BGP speaker that constructed this FC segment is sending the UPDATE message to a peer AS within the same AS confederation [RFC5065]. In all other cases, the Flags-CS flag is set to 0. The second leftmost bit (i.e., the second highest) of the Flags field is the Route_Server flag (Flags-RS). The Flags-RS flag is set to 1 to indicate that a route server adds this FC segment, but the AS number will never appear in the AS_PATH attribute. If the AS number of a router server is inserted into AS_PATH, this Flags-RS flag MUST be set to 0. The third leftmost bit (i.e., the third highest) of the Flags field is the Only_to_Customer flag (Flags-OTC). The Flags-OTC flag is set to 1 to indicate that the FC segment's issuer AS sends routes to its customer or peer. If this Flags-OTC flag is set, the next route propagation will only be permitted to the following customers. The remaining 5 bits of the Flags field are unassigned. They MUST be set to 0 by the sender and ignored by the receiver.

Signature Length (2 octets): It only contains the length of the Signature field in octets, not including other fields.

Signature (variable length): The signature content and order are Signature=ECDSA(SHA256(PASN, CASN, NASN, Prefix, Prefix Length)), where the Prefix is the IP address prefix which is encapsulated in the BGP UPDATE, i.e. NLRI, and only one prefix is used each time. When hashing and signing, the full IP address and IP prefix length are used, i.e., IPv4 uses 4 octets and IPv6 uses 16 octets.

3.2. FC Path Attribute

A detailed description of the FC Path Attribute is provided here. The FC path attribute is in Type-Length-Value format. The specification for the FC Path Attribute is provided in Figure 2.

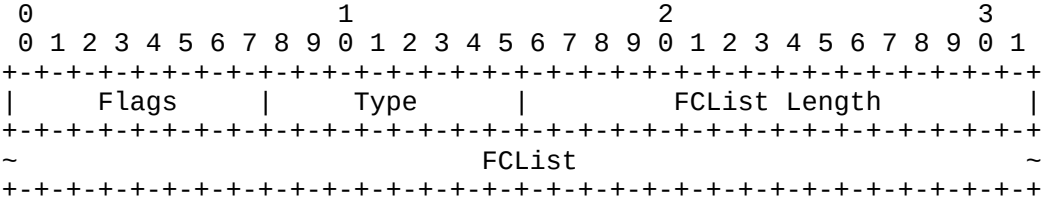

Figure 2: The structure of the FC Path Attribute

Flags (1 octet): The current value is 0b11010000, representing the FC path attribute as optional, transitive, partial, and extended-length.

Type (1 octet): The current value is TBD.

FCList Length (2 octets): The value is the total length of the FCList in octets.

FCList (variable length): The value is a sequence of FC segments, in order.

4. The FC Path Attribute in BGP UPDATE Messages

Section 4.1 specifies how a BGP speaker supporting the FC path attribute generates or modifies the FC path attribute in a BGP UPDATE message.

Section 4.2 specifies how a BGP speaker supporting the FC path attribute processes a BGP UPDATE message containing the FC path attribute upon receiving it.

4.1. Constructing the FC Path Attribute

A BGP speaker supporting the FC path attribute SHOULD generate a new FC segment or even a new FC path attribute when it propagates a route to its externel neighbors. For internal neighbors, the FC path attribute message remains unchanged.

The information protected by the signature on a FC path attribute includes the AS number of the peer to whom the UPDATE message is being sent. Therefore, if a BGP speaker supporting FC wishes to send a BGP UPDATE message to multiple BGP peers, it MUST generate a separate BGP UPDATE message containing FC path attribute for each unique peer AS to whom the UPDATE message is sent.

The BGP speaker supporting the FC path attribute follows a specific process to create the attribute for the ongoing UPDATE message. Firstly, it generates a new FC segment. If there is already an existing FC path attribute, the speaker MUST prepend the new FC segment to the FCList. Otherwise, the speaker generates the FC path attribute and inserts it into the UPDATE message.

There are three AS numbers in one FC segment. The Previous AS number (PASN) is typically set to the AS number from which the UPDATE message receives. However, if the speaker is located in the origin AS, the PASN SHOULD be filled with 0. The Nexthop AS number (NASN)

is set to the AS number of the peer to whom the route is advertised. So if there are several neighbors, the speaker SHOULD generate separate FCs for different neighbors. But it would never generate a new FC segment for the iBGP neighbor.

The Subject Key Identifier field (SKI) within the new FC segment is populated with the identifier found in the Subject Key Identifier extension of the router certificate associated with the speaker. This identifier enables others to identify the appropriate certificate to employ when verifying signatures in FC segments attached to the router advertisement.

Typically, the Flags field is set to 0, but the speaker SHOULD modify it based on section 3.1. The Algorithm ID field is set to 1, and the Signature Length field is populated with the length (in octets) of the value in the Signature field.

The Signature field in the new FC segment is a variagble length field. It contains a digital signature encapsulated in DER format that binds the prefix, its length, and triplet (PASN, CASN, NASN) to the RPKI router certificate corresponding to the FC-BGP speaker. The digital signature is computed as follows: Signature=ECDSA(SHA256(PASN, CASN, NASN, Prefix, Prefix Length)).

4.2. Processing the FC Path Attribute

AS supporting FC path attribute MUST additionally follow the instructions in this section for processing BGP UPDATE messages containing the FC path attribute, after which the speaker can continue advertising the BGP route. As a prerequisite, the recipient SHOULD have access to certificates.

First, the integrity of the UPDATE message containing the FC path attribute MUST be checked. The speaker SHOULD check the FC path attribute to ensure that the entire FC path attribute is syntactically correct, the triplet (PASN, CASN, NASN) fields in each FC segment follow the order in AS_PATH, and each FC segment contains one signature with the supported Algorithm ID.

If any of the checks for the FC path attribute fail, indicating a syntactical or protocol errors, it is considered an error. In such cases, FC speakers are REQUIRED to handle these errors using the "treat-as-withdraw" approach as defined in [RFC7607]. Otherwise, the speaker iterates through the FC segments. It SHOULD proceed to validate the signature using the supported algorithm suites. In details, it SHOULD locate the public key needed to verify the signature in the current segment, compute the digest function, and use the signature validation algorithm to verify the signature in the current segment.

If all FC segments are marked as 'Valid', then the validation algorithm terminates and the UPDATE message is deemed 'Valid'. Otherwise, the UPDATE message is deemed 'Not Valid'.

5. Security Considerations

5.1. Security Guarantees

When the FC path attribute is used in conjunction with origin validation, the following security security guarantees can be achieved: The source AS in a route announcement is authorized; BGP speakers on the AS path are authorized to propagate the route announcements; The forwarding path of packets is consistent with the routing path announced by the BGP speakers.

The FC path attribute is designed to enhance the security of control plane routing in the Internet at the network layer. Specifically, It allows an AS to independently prove its BGP routing decisions with publicly varifiable cryptography commitments, based on which any on-path AS can verify the authenticity of a BGP path. More crucially, the above security guarantees offered by the FC path attribute are binary, i.e., secure or non-secure. Instead, the security benefits are strictly monotonically increasing as the deployment rate of the FC path attribute increases.

5.2. Mitigation of Denial-of-Service Attacks

The FC path attribute involves numerous cryptographic operations, which makes BGP speakers supporting it vulnerable to Denial-of-Service (DoS) attacks. This section addresses the mitigation strategies tailored for the specific DoS threats.

To reduce the impact of DoS attacks, speakers SHOULD employ an UPDATE validation algorithm that prioritizes inexpensive checks (such as syntax checks) before proceeding to more resource-intensive operations (like signature verification).

Moreover, the transmission of UPDATE messages with the FC path attribute, which entails a multitude of signatures, is a potential vector for denial-of-service attacks. To counter this, implementations of the validation algorithm must cease signature verification immediately upon encountering an invalid signature. This prevents prolonged sequences of invalid signatures from being exploited for DoS purposes. Additionally, implementations can further mitigate such attacks by limiting validation efforts to only those UPDATE messages that, if found to be valid, would be chosen as the best path. In other words, if an UPDATE message includes a route that would be disqualified by the best path selection process for some reason (such as an excessively long AS path), it is OPTIONALLY to determine its FC path attribute validity status.

5.3. Route Server

When the Route Server populates its FC Segment into the FC path attribute, it is secure as the path is fully deployed.

When the Route Server fails to insert FC Segment, no matter whether its ASN is listed in the AS path, it is considered a partial deployment which poses a risk of path forgery.

5.4. Three AS Numbers

An FC segment contains only partial path information and FCs in the FCList are independent. To prevent BGP Path Splicing attacks, we propose to use the triplet (Previous AS Number, Current AS Number, Nexthop AS Number) to locate the pathlet information.

But if there is no previous hop, i.e., this is the origin AS that tries to add its FC segment to the BGP UPDATE message, the Previous AS Number SHOULD be populated with 0. But, carefully, AS 0 SHOULD only be used in this case.

In the context of BGP [RFC4271], to detect an AS routing loop, it scans the full AS path (as specified in the AS_PATH attribute) and checks that the autonomous system number of the local system does not appear in the AS path. As outlined in [RFC7607], Autonomous System 0 was listed in the IANA Autonomous System Number Registry as "Reserved - May be used to identify non-routed networks". So, there should be no AS 0 in the AS_PATH attribute of the BGP UPDATE message. Therefore, AS 0 could be used to populate the PASN field when no previous AS hops in the AS path.

6. IANA Considerations

This document requires the following IANA actions:

This document requests the assignment of a new attribute code described in Section 1 in the "FC Path Attributes" registry. The attribute code for this new path attribute "FC_PATH" to provide consistency between the control and data planes. This document is the reference for the new attribute.

7. 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>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5065] Traina, P., McPherson, D., and J. Scudder, "Autonomous System Confederations for BGP", RFC 5065, DOI 10.17487/RFC5065, August 2007, <https://www.rfc-editor.org/info/rfc5065>.

[RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, DOI 10.17487/RFC5492, February 2009, <https://www.rfc-editor.org/info/rfc5492>.

[RFC6472] Kumari, W. and K. Sriram, "Recommendation for Not Using AS_SET and AS_CONFED_SET in BGP", BCP 172, RFC 6472, DOI 10.17487/RFC6472, December 2011, <https://www.rfc-editor.org/info/rfc6472>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <https://www.rfc-editor.org/info/rfc6483>.

[RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, DOI 10.17487/RFC6793, December 2012, <https://www.rfc-editor.org/info/rfc6793>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

[RFC7607] Kumari, W., Bush, R., Schiller, H., and K. Patel, "Codification of AS 0 Processing", RFC 7607, DOI 10.17487/RFC7607, August 2015, <https://www.rfc-editor.org/info/rfc7607>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

[RFC8208] Turner, S. and O. Borchert, "BGPsec Algorithms, Key Formats, and Signature Formats", RFC 8208, DOI 10.17487/RFC8208, September 2017, <https://www.rfc-editor.org/info/rfc8208>.

[RFC8209] Reynolds, M., Turner, S., and S. Kent, "A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests", RFC 8209, DOI 10.17487/RFC8209, September 2017, <https://www.rfc-editor.org/info/rfc8209>.

[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>.

[RFC8635] Bush, R., Turner, S., and K. Patel, "Router Keying for BGPsec", RFC 8635, DOI 10.17487/RFC8635, August 2019, <https://www.rfc-editor.org/info/rfc8635>.

Authors' Addresses

Ke Xu
Tsinghua University
Beijing
China
Email: xuke@tsinghua.edu.cn

Xiaoliang Wang
Tsinghua University
Beijing
China
Email: wangxiaoliang0623@foxmail.com

Zhuotao Liu
Tsinghua University
Beijing
China
Email: zhuotaoliu@tsinghua.edu.cn

Qi Li
Tsinghua University
Beijing
China
Email: qli01@tsinghua.edu.cn

Jianping Wu
Tsinghua University
Beijing
China
Email: jianping@cernet.edu.cn

Yangfei Guo
Zhongguancun Laboratory
Beijing
China
Email: guoyangfei@zgclab.edu.cn

Jinsi Wu
Tsinghua University
Beijing
China
Email: wjs24@mails.tsinghua.edu.cn