SIDR Operations
Internet-Draft
Intended status: Standards Track
Expires: 23 August 2025

K. Xu
Tsinghua University
S. Jiang
Y. Guo
ZGC Laboratory
X. Wang
Tsinghua University

19 February 2025

BGP AS_PATH Verification Based on Forwarding Commitment (FC) Objects
draft-xu-sidrops-fc-verification-00

Abstract

The Forwarding Commitment (FC) is an RPKI object that attests to the complete routing intents description which an Autonomous System (AS) would obey in Border Gateway Protocol (BGP) route propagation. This document specifies an FC-based AS Path Verification methodology to mitigate, even solve, AS Path forgery and route leaks. This document also explains the various BGP security threats that FC can help address and provides operational considerations associated with FC deployment.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://FCBGP.github.io/fc-verification/draft-xu-sidrops-fc-verification.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-xu-sidrops-fc-verification/.

Discussion of this document takes place on the SIDR Operations mailing list (mailto:sidrops@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/sidrops/. Subscribe at https://www.ietf.org/mailman/listinfo/sidrops/.

Source for this draft and an issue tracker can be found at https://github.com/FCBGP/fc-verification.

Status of This Memo

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

This Internet-Draft will expire on 23 August 2025.

Copyright Notice

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) is vulnerable to route hijacks and route leaks [RFC7908]. Some existing BGP extensions can partially solve or alleviate these problems. Resource Public Key Infrastructure (RPKI) based route origin validation (RPKI-ROV) [RFC6480] [RFC6811] [RFC9319] [RFC9582] and Signed Prefix List-based Route Origin Verification (SPL-ROV) [I-D.ietf-sidrops-rpki-prefixlist] can be used to detect and filter accidental mis-originations. BGPsec is designed to provide security for the AS-path attribute in the BGP UPDATE message [RFC8205]. [RFC9234] and Autonomous System Provider Authorization (ASPA) [I-D.ietf-sidrops-aspa-profile] aim at detecting and mitigating accidental route leaks.

However, there are still some issues that need to be addressed. ASPA is a genius mechanism to verify BGP AS-path attribute content, which only stores customer-to-provider information in RPKI. Autonomous System Relationship Authorization (ASRA) has listed several security problems with ASPA in Section 2 of [I-D.geng-sidrops-asra-profile]. Though the validity of the ASPA/ASRA objects is verified, the relationship between two BGP neighbors cannot be attested. When two ASes announce mutually exclusive relationships, for example, AS A says AS B is its Provider and AS B says AS A is its Provider, no other ASes can verify their real relationships.

The Forwarding Commitment (FC) [I-D.guo-sidrops-fc-profile] is a Resource Public Key Infrastructure (RPKI) object that attests to the complete routing intents description an Autonomous System (AS) would obey in Border Gateway Protocol (BGP) route propagation.

This document specifies an FC-based AS Path Verification methodology to prevent AS path forgery in the BGP AS-path attribute of advertised routes. FC-based AS_PATH verification also detects and mitigates route leaks.

2. Requirements Language

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. Definition of Commonly Used Terms

The definitions and semantics of Forwarding Commitment (FC) provided in [I-D.guo-sidrops-fc-profile] are applied here.

* *Route is ineligible*: The term has the same meaning as in [RFC4271], i.e., "route is ineligible to be installed in Loc-RIB and will be excluded from the next phase of route selection."

* *AS-path*: This term defines a sequence of ASes listed in the BGP UPDATE AS_PATH or AS4_PATH attribute. In this document, the terms AS-path, AS_PATH, and AS4_PATH are interchangeably used.

* *TotallyValid*: This is one of the verification results of using FC objects to verify AS_PATH. This means the FCs of each AS in AS_PATH are all with the 'originASes' field.

* *VFP*: Validated FC Payload (see Section 4).

4. Forwarding Commitment (FC)

Forwarding Commitment (FC) objects encapsulate the routing intent description of an Autonomous System (AS). Unlike most RPKI-signed objects, FC objects possess a distinct design regarding verification results. Since FC objects reference Route Origin Authorizations (ROAs) within their content, the verification outcomes for FC are categorized into four distinct states: TotallyValid, Valid, Invalid, and Unknown.

It is RECOMMENDED that all routing intents be explicitly enumerated within a single FC object. However, due to the inherent complexity of routing intents, providing a comprehensive list can be challenging. Consequently, it is RECOMMENDED to include routing intents with the originASes field designated as 'NONE' when the issuer is unable to specify which routes will be propagated from previousASes to nexthopASes. It may have a few of these routingIntents with the originASes field set as 'NONE'.

In general, there exists a singular valid FC object corresponding to a specific asID. However, in instances where multiple valid FC objects containing the same asID are present, the union of the resulting routingIntent members constitutes the comprehensive set of members. This complete set, which may arise from either a single or multiple FCs, is locally maintained by a Relying Party (RP) or a compliant router. Such an object is referred to as the Validated FC Payload (VFP) for the asID.

Except for the empty originASes, there would also be empty previousASes and nexthopASes in a routing intent. It is NOT RECOMMENDED to describe routing intent without nexthopASes as this does not help verify BGP AS_PATH.

It is REQUIRED at least one routing intent description in an FC object. Otherwise, the empty FC object means no routes can be transited or transformed from this asID.

5. BGP AS_PATH Verification Algorithm Using FC

FCs describe the local routing intents of an AS. It can be used to verify the AS-path attribute in the BGP UPDATE message.

Before the AS_PATH verification procedure, it can first perform prefix origin verification with ROA-ROV defined in Section 2 of [RFC6811] or SPL-ROV defined in Section 4 of [I-D.ietf-sidrops-spl-verification].

An eBGP router that conforms to this specification MUST implement FC-based AS_PATH verification procedures specified below.

For each received BGP route:

1. Query all the FCs that are issued by the ASes that are in the AS-path attribute;

2. If all ASes on the AS-path have their FCs with the BGP AS-path conforming to all ASes routing intents and the route is also specified in the originASes field, the verification result is TotallyValid;

3. Else, if the originASes field is missing but all ASes on the AS-path have their FCs with the BGP AS-path conforming to all ASes routing intents, the verification result is Valid;

4. Else, if none of the AS on the AS path has its FC, the verification result is Unknown;

5. Else, if some of the ASes on the AS path have their FCs but others ASes do not have their FCs, the verification result is Invalid.

5.1. Mitigation Policy

The specific configuration of a mitigation policy based on AS_PATH verification using FC is at the discretion of the network operator. However, the following mitigation policy is highly recommended.

Invalid: If the AS_PATH is determined to be Invalid, then the route SHOULD be considered ineligible for route selection and MUST be kept in the Adj-RIB-In for potential future re-evaluation (see [RFC9324]).

TotallyValid, Valid, or Unknown: When a route is evaluated as Unknown (using FC-based AS_PATH verification), it SHOULD be treated at the same preference level as a route evaluated as Valid. But TotallyValid has the highest priority in BGP route selection while Valid has a second priority.

6. Operational Considerations

Multiple valid Forwarding Commitment objects which contain the same asID could exist. In such a case, the union of these objects forms the complete routing intent set of this AS. For a given asID, it is RECOMMENDED that a CA maintains a single Forwarding Commitment. If an AS holder publishes a Forwarding Commitment, then relying parties SHOULD assume that this object is complete for that issuer AS.

If one AS receives a BGP UPDATE message with the issuer AS in the AS-path attribute which cannot match any routing intents of this issuer AS, it implies that there is an AS-path forgery in this message.

7. Security Considerations

TODO Security

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[I-D.geng-sidrops-asra-profile]
Geng, N., Sriram, K., and M. Huang, "A Profile for Autonomous System Relationship Authorization (ASRA)", Work in Progress, Internet-Draft, draft-geng-sidrops-asra-profile-00, 13 October 2024, <https://datatracker.ietf.org/doc/html/draft-geng-sidrops-asra-profile-00>.

[I-D.guo-sidrops-fc-profile]
Guo, Y., Wang, X., Xu, K., liu, Z., and L. Qi, "A Profile for Forwarding Commitments (FCs)", Work in Progress, Internet-Draft, draft-guo-sidrops-fc-profile-00, 18 February 2025, <https://datatracker.ietf.org/doc/html/draft-guo-sidrops-fc-profile-00>.

[I-D.ietf-sidrops-aspa-profile]
Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-19, 6 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-19>.

[I-D.ietf-sidrops-rpki-prefixlist]
Snijders, J. and G. Huston, "A profile for Signed Prefix Lists for Use in the Resource Public Key Infrastructure (RPKI)", Work in Progress, Internet-Draft, draft-ietf-sidrops-rpki-prefixlist-04, 16 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-rpki-prefixlist-04>.

[I-D.ietf-sidrops-spl-verification]
Sriram, K., Snijders, J., and D. Montgomery, "Signed Prefix List (SPL) Based Route Origin Verification and Operational Considerations", Work in Progress, Internet-Draft, draft-ietf-sidrops-spl-verification-01, 14 December 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-spl-verification-01>.

[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/rfc/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/rfc/rfc4271>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/rfc/rfc6480>.

[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/rfc/rfc6811>.

[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/rfc/rfc8174>.

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

[RFC9234] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages", RFC 9234, DOI 10.17487/RFC9234, May 2022, <https://www.rfc-editor.org/rfc/rfc9234>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/rfc/rfc9582>.

9.2. Informative References

[RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June 2016, <https://www.rfc-editor.org/rfc/rfc7908>.

[RFC9319] Gilad, Y., Goldberg, S., Sriram, K., Snijders, J., and B. Maddison, "The Use of maxLength in the Resource Public Key Infrastructure (RPKI)", BCP 185, RFC 9319, DOI 10.17487/RFC9319, October 2022, <https://www.rfc-editor.org/rfc/rfc9319>.

[RFC9324] Bush, R., Patel, K., Smith, P., and M. Tinka, "Policy Based on the Resource Public Key Infrastructure (RPKI) without Route Refresh", RFC 9324, DOI 10.17487/RFC9324, December 2022, <https://www.rfc-editor.org/rfc/rfc9324>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

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

Shenglin Jiang
ZGC Laboratory
Beijing
China
Email: jiangshl@zgclab.edu.cn

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

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