SIDR Operations
Internet-Draft
Intended status: Standards Track
Expires: 4 June 2026

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

1 December 2025

BGP AS_PATH Verification Based on Route Path Authorizations (RPA) Objects
draft-xu-sidrops-rpa-verification-01

Abstract

The Route Path Authorizations (RPA) is an RPKI object that attests to the routing paths description which an Autonomous System (AS) would obey in Border Gateway Protocol (BGP) route propagation. This document specifies an RPA-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 RPA can help address and provides operational considerations associated with RPA 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/rpki-rpa-verification/draft-xu-sidrops-rpa-verification.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-xu-sidrops-rpa-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/rpki-rpa-verification.

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 4 June 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) is vulnerable to route hijacks and route leaks [RFC7908]. Several existing BGP extensions can mitigate these attacks to some extent. 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) [RPKI-SPL-Profile] can be used to detect and filter accidental mis-originations. BGPsec is designed to provide assurance for the AS-path attribute in the BGP UPDATE message [RFC8205]. [RFC9234] and Autonomous System Provider Authorization (ASPA) [RPKI-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. Though the validity of the ASPA 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 Route Path Authorizations (RPA) [RPKI-RPA-Profile] is a Resource Public Key Infrastructure (RPKI) object that attests to the routing paths description an Autonomous System (AS) would obey in Border Gateway Protocol (BGP) route propagation.

This document specifies an RPA-based AS Path Verification methodology to prevent AS path forgery in the BGP AS-path attribute of advertised routes. RPA-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 Route Path Authorizations (RPA) provided in [RPKI-RPA-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."

* *Weakly Valid*: This is one of the verification status of using RPA objects to verify AS_PATH, indicating that at least one AS in the path is validated as VALID by RPA, while all other ASes yield an UNKNOWN verification result.

* *VRPP*: Validated RPA Payload (see Section 4).

4. Route Path Authorizations (RPA)

Route Path Authorizations (RPA) objects encapsulate the routing paths description of an AS. Similar to most RPKI-signed objects, the verification results for RPA are classified into four distinct states: Valid, Weakly Valid, Invalid, and Unknown.

It is RECOMMENDED that all routing paths be explicitly enumerated within a single RPA object. However, due to the inherent complexity of routing paths, providing a comprehensive list can be challenging. Consequently, it is RECOMMENDED to include routing paths with the origins/prefixes field designated as 'NONE' when the issuer is unable to specify which routes will be propagated from previousHops to nextHops. It may have a few of these routePathBlocks with the origins/prefixes field set as 'NONE'.

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

Except for the empty origins, there would also be empty previousHops and nextHops in a routing path. It is NOT RECOMMENDED to describe routing path without nextHops as this does not help verify BGP AS_PATH.

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

5. AS_PATH Verification Using RPA

RPAs describe the local routing paths of an AS. They can be used to verify the AS_PATH attribute in BGP UPDATE messages.

Upon receiving a BGP UPDATE message, the AS_PATH verification procedure is initiated. This process involves querying the corresponding RPA for each AS along the path individually. If the prefixes field of an RPA object is non-empty, prefix matching is performed. Furthermore, if the origins field is present, additional validations are carried out using ROA-based Route Origin Validation (ROA-ROV) as defined in Section 2 of [RFC6811] and SPL-ROV as defined in Section 4 of [RPKI-SPL-Verification].

An eBGP router that conforms to this specification MUST implement RPA-based AS_PATH verification procedures defined below. These procedures operates in a two-stage process:

1. Per-AS Verification: At the first stage, each AS in the AS_PATH is evaluated individually based on its corresponding RPA object, if available. This stage validates whether each AS’s declared routing path is consistent with the received AS_PATH attributes.

2. Path-Level Verification: At the second stage, the system derives an overall path verification status by aggregating the outcomes of the per-AS verifications. The final status reflects the consistency and completeness of the entire path with respect to the available RPAs.

5.1. Per-AS Verification Algorithm

The verification algorithm is applied to each individual AS in the AS_PATH of the received BGP UPDATE message. For each AS, its corresponding RPA object is examined to verify attributes such as prefix scope, authorized neighbors, and origin declaration. The verification result for each AS is one of: Valid, Invalid, or Unknown, depending on the presence and content of the RPA and its alignment with the BGP announcement.

1. Query the RPA associated with AS.

2. If RPA is not available, then set AS verification result is Unknown.

3. Perform authorized neighbors matching against the AS_PATH. If RPA.previousHops or RPA.nextHops do not match the AS_PATH context, set AS verification result is Invalid.

4. If RPA.prefixes is non-empty, perform prefix matching with the UPDATE message.

5. If RPA.origins is non-empty, perform ROA-ROV and SPL-ROV validation.

6. If both prefix and origin checks succeed, set AS verification result is Valid.

7. If either check fails, set AS verification result is Invalid.

8. Else, set AS verification result is Unknown.

5.2. Path-Level Verification Algorithm

This process determines whether the sequence of ASes in the AS_PATH attribute conforms to the collectively declared routing paths published in RPAs. By aggregating the per-AS verification results, the algorithm computes a comprehensive path verification result for each received BGP route.

1. Let valid_count is set equal to number of ASes with Valid. Let invalid_count is set equal to number of ASes with Invalid. Let unknown_count is set equal to number of ASes with Unknown.

2. If valid_count == 0 AND invalid_count == 0, then the verification result is Unknown.

3. Else, if invalid_count == 0 AND unknown_count == 0, then the verification result is Valid.

4. Else, if valid_count >= 1 AND invalid_count == 0, then the verification result is Weakly Valid.

5. Else, if invalid_count >= 1, then the verification result is Invalid.

6. Else, the verification result is Unkown.

5.3. Mitigation Policy

The specific configuration of a mitigation policy based on AS_PATH verification using RPA 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]).

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

6. Operational Considerations

Multiple valid RPA objects that contain the same asID could exist. In such a case, the union of these objects forms the routing path set of this AS. For a given asID, it is RECOMMENDED that a CA maintains a single RPA. If an AS holder publishes an RPA, 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 path 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

[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>.

[RPKI-RPA-Profile] Guo, Y. B., 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>.

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>.

[RPKI-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-20, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-20>.

[RPKI-SPL-Profile]
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>.

[RPKI-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-02, 16 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-spl-verification-02>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

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

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

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

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