sidrops
Internet-Draft
Intended status: Standards Track
Expires: 18 December 2025

K. Sriram
USA NIST
J. Snijders
Fastly
D. Montgomery
USA NIST

16 June 2025

Signed Prefix List (SPL) Based Route Origin Verification and Operational Considerations
draft-ietf-sidrops-spl-verification-02

Abstract

The Signed Prefix List (SPL) is an RPKI object that attests to the complete list of prefixes which an Autonomous System (AS) may originate in the Border Gateway Protocol (BGP). This document specifies an SPL-based Route Origin Verification (SPL-ROV) methodology and combines it with the ROA-based ROV (ROA-ROV) to facilitate an integrated mitigation strategy for prefix hijacks and AS forgery. The document also explains the various BGP security threats that SPL can help address and provides operational considerations associated with SPL-ROV deployment.

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 18 December 2025.

Copyright Notice

Table of Contents

1. Introduction

The Signed Prefix List (SPL) [I-D.ietf-sidrops-rpki-prefixlist] is a Resource Public Key Infrastructure (RPKI) object that attests to the complete list of prefixes which an Autonomous System (AS) may originate in the Border Gateway Protocol (BGP). This document specifies an SPL-based Route Origin Verification (SPL-ROV) procedure and how it can be combined with ROA-based ROV (ROA-ROV) [RFC6811][RFC9319] to facilitate an integrated mitigation strategy for prefix hijacks, AS forgery, and reduction of attack surface for forged-origin prefix hijacks. An AS forgery occurs when an offending AS illegitimately inserts another AS (victim AS) as the origin in a BGP announcement (prefix may belong to a third party or the offender). A forged-origin prefix hijack occurs when an offending AS makes a BGP announcement with illegitimate insertion of a {prefix, origin AS} tuple that is Valid per ROA-ROV [RFC7115][RFC9319]. The various BGP security threats that SPL-ROV helps to address are described in Section 6. Operational considerations associated with

SPL-ROV are discussed in Section 7.

The verification procedures described in this document MUST be applied to BGP routes with {AFI, SAFI} combinations {AFI 1 (IPv4), SAFI 1} and {AFI 2 (IPv6), SAFI 1} [IANA-AF] [IANA-SAF]. The procedures MUST NOT be applied to other address families by default.

1.1. 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.

2. Terminology and List of Acronyms

The following list includes the terms used with special meanings and acronyms.

* "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."

* SPL: Signed Prefix List (see [I-D.ietf-sidrops-rpki-prefixlist]).

* VSP: Validated SPL Payload (see Section 3).

* ROA: Route Origin Authorization (see [RFC6811]).

* ROA-ROV: ROA-based Route Origin Verification (see Section 4).

* SPL-ROV: SPL-based Route Origin Verification (see Section 4).

* RP: Relying Party (see [RFC6484]).

3. Signed Prefix List (SPL) and Validated SPL Payload (VSP)

The definition and semantics of Signed Prefix List (SPL) are provided in [I-D.ietf-sidrops-rpki-prefixlist] apply here. Additional clarification is that the SPL object does not implicitly permit a more-specific prefix subsumed by a listed IP address prefix to be originated by the subject AS listed in it. For any such more-specific prefix to be permitted by the SPL object, it must be explicitly listed in the list of IP address prefixes.

Normally there would be a single valid Signed Prefix List (SPL) object for a given asID [I-D.ietf-sidrops-rpki-prefixlist]. However, if multiple valid SPL objects which contain the same asID exist, then union of the resulting address prefix members forms the complete set of members. The complete set (resulting from a single or multiple SPLs) is locally stored by a Relying Party (RP) or compliant router, and such an object is called the Validated SPL Payload (VSP) for the asID in consideration. For a given asID, there may be only a valid SPL object with zero prefixes listed. By creating such an empty SPL object, the subject AS is declaring that it does not originate any prefixes. For an empty SPL, the corresponding VSP conveys 'Empty' in place of the set of prefixes [I-D.ietf-sidrops-rpki-prefixlist].

4. Route Origin Verification Algorithms Using ROA and SPL

SPLs provide a second means to perform route origin verification (ROV) based upon RPKI data. In this document, we refer to the ROV based upon ROA data as ROA-ROV and the ROV based upon SPL data (algorithm described below) as SPL-ROV.

This document makes no changes to the ROA-ROV procedure defined in Section 2 of [RFC6811]. The SPL-ROV procedure described below is designed to augment and integrate with the existing ROA-ROV procedures. The ROA-ROV and SPL-ROV procedures produce independent verification results referred to as ROA-ROV-state and SPL-ROV-state, respectively.

An eBGP router that conforms to this specification MUST implement both the ROA-ROV and SPL-ROV procedures specified below.

For each received BGP route:

1. Set the ROA-ROV-state = the outcome (NotFound, Valid, or Invalid) of the route origin verification procedure in Section 2 of [RFC6811].

2. If the route contains an AS_SET, then set the SPL-ROV-state = Invalid and stop.

3. Else, if the route's origin AS does not have a VSP, then set the SPL-ROV-state = NotFound and stop.

4. Else, if the route's origin AS's VSP includes the route prefix, then set the SPL-ROV-state = Valid and stop.

5. Else, set the SPL-ROV-state = Invalid and stop.

5. Mitigation Policy

The specific configuration of a mitigation policy is at the discretion of the network operator. However, the following mitigation policy is highly recommended.

If either the route's SPL-ROV-state or ROA-ROV-state = Invalid (Section 4), then the route SHOULD be considered ineligible for route selection (see Section 2) but MUST be kept in the Adj-RIB-In for potential future re-evaluation (see [RFC9324]). To be clear, the above applies when either or both of the two ROV states is (or are) Invalid. Routes with all other combinations of the SPL-ROV and ROA-ROV states (i.e., Valid-Valid, Valid-NotFound, NotFound-Valid, NotFound-NotFound) SHOULD be considered eligible for best path selection and SHOULD get the same preference level relative to each other (assuming other path properties are equal).

For visualization purposes, Table 1 below lists all possible combinations of the ROA-ROV and SPL-ROV states and the associated recommendations for the route's eligibility for path selection.

Index	ROA-ROV-state	SPL-ROV-state	Route Selection
1	Valid	Valid	Eligible
2	Valid	NotFound	Eligible
3	Valid	Invalid	Ineligible
4	NotFound	Valid	Eligible
5	NotFound	NotFound	Eligible
6	NotFound	Invalid	Ineligible
7	Invalid	Valid	Ineligible
8	Invalid	NotFound	Ineligible
9	Invalid	Invalid	Ineligible

Table 1

6. BGP Security Threats Addressed by SPL-ROV

The BGP security threats addressed by deploying SPL-ROV together with ROA-ROV (Section 4) and the mitigation policy (Section 5) are discussed below.

1. *AS Forgery While Hijacking an ROA-ROV-NotFound Prefix:* If AS A creates an SPL, it is protected by SPL-ROV in case an offending AS X inserts AS A as the origin AS and announces a third-party prefix not covered by a ROA.

2. *AS Forgery Together with a Conflicting ROA:* A conflicting ROA is one which attests the origination of a prefix from an AS but the AS has not included the specific prefix in its SPL. Consider the scenario in which AS A creates a Signed Prefix List. In this case, AS A is protected by SPL-ROV if an offending AS X inserts AS A as the origin AS and announces a prefix for which AS X holds an RPKI certificate and has signed a conflicting ROA showing AS A as the origin.

3. *AS Accidentally Strips AS_PATH and Mis-Originates Prefixes:* An AS learns a route from an eBGP neighbor and announces the prefix to another eBGP neighbor as if it is being originated by it (i.e., strips the received AS_PATH and re-originates the prefix). This can be called a re-origination or mis-origination attack (also see Type 5 route leak in [RFC7908]). This attack has been seen to happen in practice due to malfunctioning route optimizers. It can be mitigated at neighboring ASes by SPL-ROV if the AS in consideration has registered an SPL.

4. *Attack Surface Reduction:* Often a prefix owner includes more prefixes and/or more more-specific prefixes (using maxLength or otherwise) in their ROA but has no plans to announce some or many of them. Such overly broad ROAs create a larger attack surface for forged-origin prefix and/or subprefix hijacks (Section 1). Creation of an SPL and the deployment of SPL-ROV can reduce this attack surface by effectively restricting the broad set of prefixes announcements authorized by the ROA to the subset of prefixes originated by the origin AS (i.e., prefixes in its VSP).

5. *AS can declare itself "Not Originating Prefixes in the Internet":* An SPL can be created with an empty prefix list in it. In doing this, the AS is asserting that it is not originating any prefixes in the Internet. Any route showing this AS as the origin AS is Invalid per SPL-ROV.

7. Operational Considerations

7.1. Considerations when Prefix Owner Splits a Prefix

A prefix owner with a prefix listed in the SPL of an AS may one day decide to split its prefix and announce only a more-specific prefix (subsumed under the prefix) from the AS in consideration. This operation needs to be managed carefully by applying the make-before-break principle. When notified of the intent, the AS must update its SPL to add the more-specific prefix while maintaining the original prefix. However, the updated SPL will take time to propagate to the RPs throughout the Internet. So, the AS must continue to announce the original prefix as well as the more-specific prefix for at least a period greater than the estimated propagation time of the updated SPL. At a later time, the less specific prefix may be removed from the AS's SPL. The prefix owner should be kept informed about the operational procedure so the expectations can be properly managed.

7.2. Considerations when Prefix Owner Has a New Prefix

A prefix owner with a new prefix may request the AS operator with an SPL to announce it. The AS operator SHOULD recommend the prefix owner to create a ROA for the new prefix. The AS operator MUST update its SPL to add the new prefix. Ubiquitous BGP propagation of the routes based upon the new prefix cannot be achieved until the updated SPL has propagated to RPs throughout the Internet. AS operators that make such SPL updates may choose to delay announcement of the new prefix to minimize triggering SPL-ROV Invalids at down-path ASes.

7.3. Avoidance of Discrepancies in the SPL

A prefix owner may dispute with the originating AS that its prefix has not been included in the AS's SPL. This can happen due to miscommunication or operational errors at the AS. A compliant AS should have appropriate operational processes to avoid such discrepancies and fix any such issues expeditiously.

7.4. DoS/DDoS Mitigation Service Provider

An AS may have a DoS/DDoS mitigation service provider (MSP) to defend against attacks targeting systems within its originated address space. Such an AS may request the MSP to include the prefixes contracted for the protection service to be included in the MSP AS's SPL. The prefixes under such a contract would be typically more-specific prefixes than the AS's normal announcements. With such an SPL in place, in the event of an attack, the MSP AS can announce the more-specific prefixes for mitigation purposes and they will be Valid per SPL-ROV. It is assumed that appropriate ROAs are also registered in advance so that the announcements are Valid per ROA-ROV as well

[RFC9319].

8. IANA Considerations

This document has no IANA considerations.

9. Security Considerations

In the SPL profile specification [I-D.ietf-sidrops-rpki-prefixlist], it is highly RECOMMENDED that an AS should only maintain one SPL that contains all the prefixes originated or intended to be originated by that AS. If an operator chooses to maintain multiple SPL objects (each with only a subset of the prefixes that could be originated by the AS), then consideration must be given to the risk imposed in scenarios in which an RP might receive some but not all of the SPL objects. Given the semantics of the SPL data as a comprehensive permit list for an AS's BGP originations, receiving some, but not all, SPL data of an AS can result in unintended route filtering and potential loss of reachability.

10. References

10.1. Normative References

[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>.

[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>.

[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>.

[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>.

[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/info/rfc9324>.

10.2. Informative References

[IANA-AF] IANA, "Address Family Numbers", <https://www.iana.org/assignments/address-family-numbers/address-family-numbers.xhtml>.

[IANA-SAF] IANA, "Subsequent Address Family Identifiers (SAFI) Parameters", <https://www.iana.org/assignments/safi-namespace/safi-namespace.xhtml>.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, DOI 10.17487/RFC6484, February 2012, <https://www.rfc-editor.org/info/rfc6484>.

[RFC7115] Bush, R., "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", BCP 185, RFC 7115, DOI 10.17487/RFC7115, January 2014, <https://www.rfc-editor.org/info/rfc7115>.

[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/info/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/info/rfc9319>.

Authors' Addresses

Kotikalapudi Sriram
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America
Email: ksriram@nist.gov

Job Snijders
Fastly
Amsterdam
Netherlands
Email: job@fastly.com

Doug Montgomery
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America
Email: dougm@nist.gov