Workgroup:
Internet Engineering Task Force (IETF)
Internet-Draft:
draft-sriram-sidrops-sav-using-aspa-roa-00
Updates: RFC8704 (if approved)
Published: 15 June 2022
Intended Status: Best Current Practice
Expires: 17 December 2022
Authors: K. Sriram I. Lubashev D. Montgomery
USA NIST Akamai USA NIST

Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)

Abstract

Designing an efficient source address validation (SAV) filter requires minimizing false positives (i.e., avoiding dropping legitimate traffic) while maintaining directionality (see RFC8704). This document advances the technology for SAV filter design through a method that makes use of BGP UPDATE messages, Autonomous System Provider Authorization (ASPA), and Route Origin Authorization (ROA). The proposed method's name is abbreviated as BAR-SAV. BAR-SAV can be used by network operators to derive more robust SAV filters and thus improve network resilience.

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 17 December 2022.

Copyright Notice

Table of Contents

1. Introduction

Spoofed source addresses are often used in Denial of Service (DoS) and Distributed DoS (DDoS) attacks. Source address validation (SAV) filtering is used to drop packets with spoofed source addresses (see BCP 84 [RFC3704] [RFC8704]). A detailed review of unicast Reverse Path Forwarding (uRPF) techniques for SAV is provided in [RFC8704]). Also, [RFC8704] describes enhanced feasible-path uRPF (EFP-uRPF) methods that aim to minimize false positives (i.e., avoid dropping legitimate traffic) while maintaining directionality (see definitions in [RFC3704]).

New technology for securing the Border Gateway Protocol (BGP) [RFC4271] using Resource Public Key Infrastructure (RPKI) [RFC6480] is seeing increasing adoption. Two of the currently existing or proposed types of signed objects in the RPKI can be leveraged for a more accurate SAV filter design as well. These are the Route Origin Authorization (ROA) and the Autonomous System Provider Authorizations (ASPA) objects. A ROA is a cryptographically signed attestation by an IP address-resource holder listing their prefixes that are authorized to be originated in BGP by a specific autonomous system (AS) [RFC6482]. ROAs are currently used for Route Origin Validation (ROV) [RFC6811]. An ASPA is a cryptographically signed attestation by an AS listing its transit provider AS numbers (ASNs) [I-D.ietf-sidrops-aspa-profile]. The ASPA data is designed to be

used for a form of AS path validation that can detect and mitigate route leaks [I-D.ietf-sidrops-aspa-verification] [sriram1] [sriram2]. See [RFC7908] for the definition of route leaks.

This document advances the technology for SAV filter design using methods that make use of ASPA, ROA, and/or BGP UPDATE data. A method is presented in Section 3 that makes use of only ASPA and ROA data to design the SAV filter. This method is for use in the future when the adoption of ROA and ASPA is considered to be ubiquitous. However, for use in the period before that, another method for SAV is presented in Section 4 that makes complementary use of BGP UPDATE messages along with ASPA and ROA data. Accordingly, the latter method's name is abbreviated as BAR-SAV. It is hoped that just as the adoption of ROAs is growing at present [Monitor], the adoption of ASPA will also gain momentum in the near future. The BAR-SAV method additionally incorporates a refined version of Algorithm A of the EFP-uRPF technique (Section 3.1 of [RFC8704]). BAR-SAV can be used by network operators to derive more robust SAV filters and thus improve network resilience.

The focus of this document is on the design of ingress SAV filters for an interface facing a customer or lateral peer AS. The same procedure applies in both cases (Section 2).

The reader is encouraged to be familiar with [RFC8704], [RFC6811], and [I-D.ietf-sidrops-aspa-profile].

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. Same Procedure Applies to Customers and Lateral Peers

The same procedure applies for the construction of a permissible ingress SAV filter for a customer or lateral peer interface. Customers and lateral peers should only transmit data packets with source addresses belonging to only the prefixes that are authorized to be used by the ASes in their respective customer cones (CC). The CC includes the AS belonging to the customer or lateral peer.

3. SAV Using ASPA and ROA (Procedure X)

The method/procedure (called Procedure X) described in this section is for future scenarios when ASPA and ROA adoption is ubiquitous. In that scenario, robust SAV filters can be generated from the RPKI information (ASPA and ROA data) alone. The procedure is applicable

for ingress SAV filter design for customer and lateral peer interfaces. An ISP may use Procedure X on customer interfaces if it requires all its customers to register ROAs and ASPAs.

A description of Procedure X (one that makes use of only ASPA and ROA data):

- Step A: Compute the set of ASNs in the Customer's or Lateral Peer's customer cone using ASPA data.

- Step B: Compute from ROA data the set of unique prefixes authorized to be announced by the ASNs found in Step A. Keep only the unique prefixes. This set is the permissible prefix list for SAV for the interface in consideration.

A detailed description of Procedure X is as follows:

1. Let the Customer or Lateral Peer ASN be denoted as AS-k.

2. Let i = 1. Initialize: AS-set S(1) = {AS-k}.

3. Increment i to i+1.

4. Create AS-set S(i) of all ASNs whose ASPA data declares at least one ASN in AS-set S(i-1) as a Provider.

5. If AS-set S(i) is null, then set i_max = i - 1 and go to Step 6. Else, go to Step 3.

6. Form the union of the sets, S(i), i = 1, 2, ..., i_max, and name this union as AS-set A.

7. Select all ROAs in which the authorized origin ASN is equal to any ASN in AS-set A. Form the union of the sets of prefixes listed in the selected ROAs. Name this union set of prefixes as P-set.

8. Apply P-set as the list of permissible prefixes for SAV.

4. SAV using BGP UPDATE Messages, ASPA, and ROA (BAR-SAV)

SAV using BGP UPDATE Messages, ASPA, and ROA (BAR-SAV) is described in this section and is meant for the period when there is a partial deployment of ROAs and ASPAs. To compensate for incomplete RPKI information, BAR-SAV augments ASPA data with BGP UPDATE AS_PATH data for discovering CC ASes, and it augments ROA data with BGP UPDATE data for discovering all prefixes associated with ASes in the CC. The details of this procedure are described below.

BAR-SAV additionally incorporates a refined version of Algorithm A of EFP-uRPF (Section 3.1 of [RFC8704]). Algorithm A in [RFC8704] picked only the originating ASes from AS_PATHs received on the customer or lateral peer interface in consideration and included them for SAV filter computation. The variant of Algorithm A in [RFC8704] used here includes all ASes in the AS_PATHs for the SAV filter computation. Unless there is a route leak [RFC7908], each AS is a customer of the AS added next in AS_PATHs of BGP UPDATE messages received from a customer or lateral peer. Further customer-provider AS relations within the CC are discovered by examining all unique ASes in the AS_PATHs in BGP UPDATEs received on all interfaces (from transit providers, customers, lateral peers, and IBGP peers). This is described in the step-by-step procedure later in this section.

Note that if a multi-homed AS is present in an above-mentioned AS_PATH and did not originate any prefix in the CC in consideration but originated a prefix into an overlapping neighboring CC, then the AS and prefix will still be detected and included in the design of the SAV filter. This improves the accuracy of the SAV filter in the BAR-SAV method in comparison to Algorithm A in [RFC8704].

One should not compute a customer cone by separately processing ASPA data and AS_PATH data and then merging the two sets of ASes at the end. Doing so is likely to miss ASes from the customer cone. Instead, both ASPAs and AS_PATHs should be used to iteratively expand the discovered customer cone. When new ASes are discovered, both ASPA and AS_PATH data should be used to discover customers of those ASes. This process is repeated for newly discovered customer ASes until there are no new ASes to be found.

If a transit provider-to-customer relationship, e.g., from AS X to AS Y, is deduced from AS_PATH data but the ASPA data contradicts it (i.e., AS Y has ASPA and it does not include AS X as a transit provider), then the ASPA data prevails, and AS Y must not be considered to be a customer of X. This design principle is reflected in Step 5 of the procedure described below. (Please see discussion about route leaks in Section 7.)

A detailed description of the BAR-SAV procedure is as follows:

1. Let the Customer or Lateral Peer ASN be denoted as AS-k.

2. Let i = 1. Initialize: AS-set Z(1) = {AS-k}.

3. Increment i to i+1.

4. Create AS-set A(i) of all ASNs whose ASPA data declares at least one ASN in AS-set Z(i-1) as a Provider.

5. Create AS-set B(i) of all "non-ASPA" customer ASNs each of which is a customer of at least one ASN in AS-set Z(i-1) according to unique AS_PATHs in Adj-RIBs-In [RFC4271] of all interfaces at the BGP speaker computing the SAV filter. "Non-ASPA" ASN are ASNs that declare no provider in ASPA data.

6. Form the union of AS-sets A(i) and B(i) and call it AS-set C. From AS-set C, remove any ASNs that are present in Z(j), for j=1 to j=(i-1). Call the resulting set Z(i).

7. If AS-set Z(i) is null, then set i_max = i - 1 and go to Step 8. Else, go to Step 3.

8. Form the union of the AS-sets, Z(i), i = 1, 2, ..., i_max, and name this union as AS-set D.

9. Select all ROAs in which the authorized origin ASN is in AS-set D. Form the union of the sets of prefixes listed in the selected ROAs. Name this union set of prefixes as Prefix-set P1.

10. Using the routes in Adj-RIBs-In of all interfaces, create a list of all prefixes originated by any ASN in AS-set D. Name this set of prefixes as Prefix-set P2.

11. Form the union of Prefix-sets P1 and P2. Apply this union set as the list of permissible prefixes for SAV.

5. Operational Recommendations

Network operators SHOULD implement the BAR-SAV method (Section 4) for computing the permissible ingress prefix list for SAV on interfaces facing customers and lateral peers. BAR-SAV offers immediate incremental benefits to early adopters.

The operational recommendations provided in Section 3.2 of [RFC8704] are applicable and helpful for BAR-SAV (Section 4). Since Procedure X (Section 3) and the BAR-SAV procedure (Section 4) benefit from the registration of ROAs, network operators are RECOMMENDED to register ROAs and enable ROV in their ASes. When ASPA becomes available, network operators are also RECOMMENDED to register ASPAs at that time.

The registration of ROAs and ASPAs helps with the detection and inclusion of otherwise hidden prefixes in the permissible list for SAV. As mentioned earlier, prefixes hidden in other techniques often arise from the use of multi-homing in conjunction with limited propagation of prefixes in a given CC (for example, by attaching NO_EXPORT to all prefixes announced from a customer AS to a transit

provider AS). In these situations, the registration of ASPAs helps improve the accuracy of SAV.

5.1. Considerations for the CDN and DSR Scenario

Direct Server Return (DSR) is a common asymmetric routing scenario that is not supported by existing BCP-84 uRPF [RFC3704] and EFP-uRPF [RFC8704] SAV methods. DSR is commonly used by Content Delivery Networks (CDNs) that wish to use anycast service addresses but deliver data from edge locations that do not announce anycast addresses.

For example, in Figure 1, the CDN announces an anycast prefix P3 (from AS3) from a well-connected location with CDN control infrastructure. When a User from prefix P1 (AS1) establishes a connection to the anycast address and requests an object, an Anycast Server at the CDN may determine that the best location to serve the object is an Edge Server in a location close to the User. The Edge Server is reachable only via prefix P2 (AS2). The Anycast Server can forward packets arriving from the User to the Edge Server (via IP-IP tunneling or similar means), but the bulk data transmission would need to happen directly from the Edge Server to the User with an anycast source address (a P3 address).

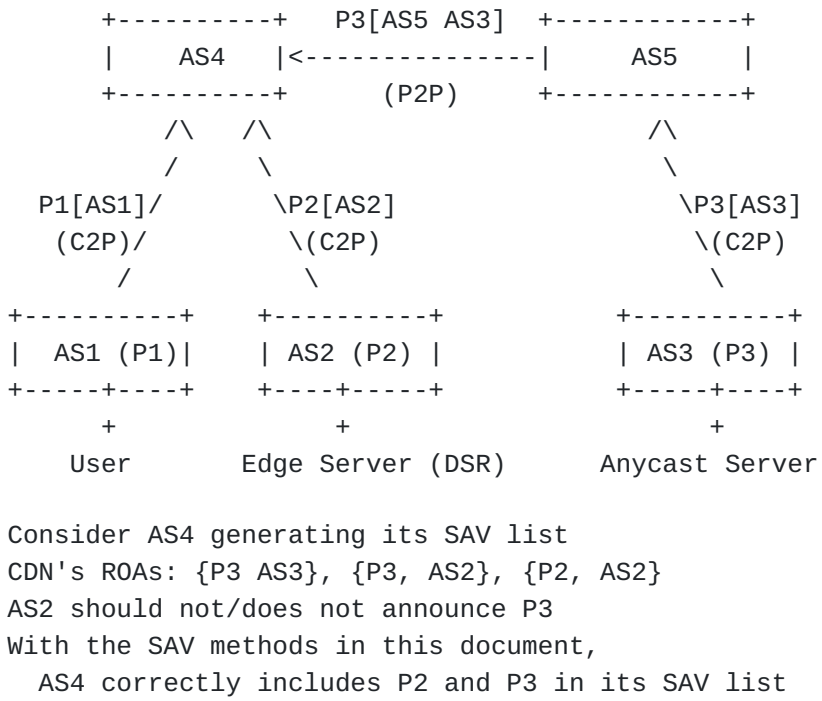

Figure 1: Illustration of how the solution functions for the CDN/DSR scenario.

Existing SAV methods of [RFC3704] and EFP-uRPF [RFC8704] would not allow AS4 to include P3 as a legitimate SA prefix on the interface to AS2. However, if the CDN (owner of prefix P3) registers a ROA object authorizing AS2 to originate P3, and AS4 uses an SAV procedure specified in this draft, then AS4 will use that ROA object to include P3 as a valid source prefix for the AS2 customer interface. The CDN may never want to announce a route to P3 from AS2, but the existence of this ROA would result in the construction of an SAV filter that would permit AS2 to send data packets with source addresses belonging to P3.

The CDN example above is just one DSR scenario. There are other cloud-based DSR scenarios that include low-latency gaming, mobile roaming, corporate networks of global enterprises, and others.

Recommendation: In a DSR scenario, a network operator SHOULD register ROAs authorizing edge server ASes to announce anycast service prefixes. This is in addition to registering a ROA authorizing the anycast server AS to announce the anycast prefix.

6. IANA Considerations

This document includes no request to IANA.

7. Security Considerations

The security considerations described in [RFC8704], [RFC6811], and [I-D.ietf-sidrops-aspa-profile] also apply to this document.

The security and robustness of BAR-SAV are strengthened by supporting mechanisms for detecting and dropping routes that are misoriginations or leaks. It is advised that the BGP UPDATEs received at BGP speakers are vetted using ROV (using ROAs and/or trusted IRR route objects) and prefix filtering (see [RFC6811] [RFC7454] [NIST-800-189]). It is also advised that one or more of the available methods to prevent, detect, and mitigate route leaks are also deployed (e.g., [RFC9234] [I-D.ietf-grow-route-leak-detection-mitigation] [I-D.ietf-sidrops-aspa-verification] [sriram1] [sriram2]).

8. References

8.1. Normative References

[I-D.ietf-sidrops-aspa-profile]
Azimov, A., Uskov, E., Bush, R., Patel, K., Snijders, J., and R. Housley, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-07, 31 January 2022, <https://

datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-07>.

[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>.

[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>.

[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>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <https://www.rfc-editor.org/info/rfc8704>.

8.2. Informative References

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and J. Snijders, "Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-08, 25 August 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-08>.

[I-D.ietf-grow-route-leak-detection-mitigation] Sriram, K. and A. Azimov, "Methods for Detection and Mitigation of BGP Route Leaks", Work in Progress, Internet-Draft, draft-ietf-grow-route-leak-detection-mitigation-07, 26 April 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-route-leak-detection-mitigation-07>.

[sriram1] Sriram, K. and J. Heitz, "On the Accuracy of Algorithms for ASPA Based Route Leak Detection", IETF SIDROPS Meeting, Proceedings of the IETF 110, March 2021, <https://datatracker.ietf.org/meeting/110/materials/slides-110-sidrops-sriram-aspa-alg-accuracy-01>.

[sriram2] Sriram, K., "ASPA Verification Procedures: Enhancements and RS Considerations", IETF SIDROPS Meeting, Proceedings of the IETF 113, March 2022, <https://datatracker.ietf.org/meeting/113/materials/slides-113-sidrops-aspa-verification-procedures-01>.

[Monitor] "NIST RPKI Monitor", National Institute of Standards and Technology, accessed June 2022, <https://rpki-monitor.antd.nist.gov/>.

[NIST-800-189] Sriram, K. and D. Montgomery, "Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation", NIST Special Publication, NIST SP 800-189, December 2019, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf>.

[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/info/rfc6480>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

[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>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454, February 2015, <https://www.rfc-editor.org/info/rfc7454>.

[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>.

[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/info/rfc9234>.

Acknowledgements

The authors would like to thank Oliver Borchert for comments and discussion.

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

Igor Lubashev
Akamai Technologies
145 Broadway
Cambridge , MA 02142
United States of America

Email: ilubashe@akamai.com

Doug Montgomery
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America

Email: dougm@nist.gov