Network Working Group
Internet-Draft
Intended status: Informational
Expires: 11 January 2023

J. Wu
D. Li
L. Qin
Tsinghua University
M. Huang
N. Geng
Huawei
10 July 2022

Source Address Validation in Inter-domain Networks (Inter-domain SAVNET) Gap Analysis, Problem Statement and Requirements

draft-wu-savnet-inter-domain-problem-statement-00

Abstract

Source Address Validation in Inter-domain Networks (Inter-domain SAVNET) focuses on narrowing the technical gaps of existing source address validation (SAV) mechanisms in inter-domain scenarios. This document provides a gap analysis of existing SAV efforts, describes the problem statement based on the analysis results, and concludes the requirements for improving inter-domain SAV.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 8174 [RFC8174].

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 11 January 2023.

Table of Contents

1. Introduction

Source address validation in inter-domain networks (Inter-domain SAVNET) is vital to mitigate source address spoofing between ASes. Inter-domain SAV is essential to the Internet security [RFC5210]. Many efforts have been taken on the tasks of inter-domain SAV.

Ingress filtering [RFC2827] [RFC3704] is a typical method of inter-domain SAV. Strict uRPF [RFC3704] reversely looks up the FIB table and requires that the valid incoming interface must be the same interface which would be used to forward traffic to the source address in the FIB table. Feasible-path uRPF (FP-uRPF) [RFC3704],

taking a looser SAV than strict uRPF, is designed to add more alternative valid incoming interfaces for the source address. To be more flexible about directionality, RFC8704 [RFC8704] recommends that i) the loose uRPF method which loses directionality completely SHOULD be applied on lateral peer and transit provider interfaces, and that ii) the Enhanced FP-uRPF (EFP-uRPF) method with Algorithm B, looser than strict uRPF, FP-uRPF, and EFP-uRPF with Algorithm A, SHOULD be applied on customer interfaces. Routers deploying EFP-uRPF accept a data packet from customer interfaces only when the source address of the packet is contained in that of the customer cone.

Despite the diversity of inter-domain SAV mechanisms, there are still some points that are underconsidered but important for enhancing Internet security. Moreover, in the currently focused SAV work scope, these mechanisms may lead to improper permit or improper block problems in some scenarios.

This document does an analysis of the existing inter-domain SAV mechanisms and answers: i) what are the technical gaps, ii) what are the major problems needing to be solved, and iii) what are the potential directions for further enhancing inter-domain SAV.

2. Terminology

SAV: Source Address Validation, i.e., validating the authenticity of a packet's source IP address.

SAV rule: The filtering rule generated by inter-domain SAV mechanisms that determines valid incoming interfaces for a specific source prefix.

SAV table: The data structure that stores SAV rules on the data plane. The router queries its local SAV table to validate the authenticity of source addresses.

Improper block: Cases when packets with legitimate source addresses

are improperly blocked.

Improper permit: Cases when packets with spoofed source addresses are improperly permitted.

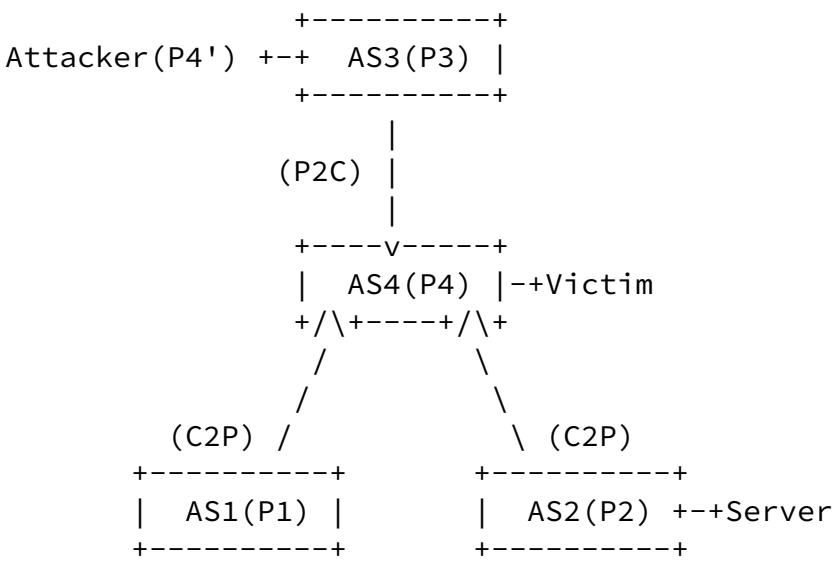
3. Gap Analysis

3.1. Weak Downstream Checking

Existing inter-domain SAV mechanisms are diverse and designed for different scenarios. However, some points are underconsidered and induce vulnerabilities to source address anti-spoofing work.

Ingress filtering mechanisms like strict uRPF are only recommended to be implemented at the edge of single-homed stub ASes. This kind of implementation aims to prevent the deployed network from sending source address spoofed packets to attack outside ASes, but not to protect the deployed network from externally injected attacks.

EFP-uRPF can be implemented at non-stub ASes, but it is only recommended at customer interfaces due to its accuracy limitations. While at provider and peer interfaces, loose uRPF is recommended. It is essentially performing ingress filtering at a higher aggregation point, which aims to restrain the behavior of ASes in the customer cone, not to protect ASes in the customer cone from externally injected attacks.



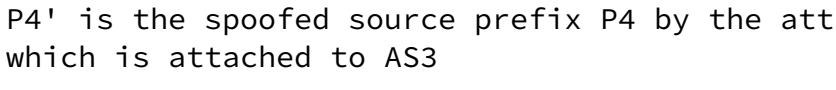


Figure 1: A reflection attack scenario

Figure 1 shows a reflection attack scenario. AS 3 is the provider of AS 4. AS 4 is the provider of AS 1 and AS 2. Strict uRPF/FP-uRPF/ EFP-uRPF are deployed at AS 4's customer interfaces, and loose uRPF is implemented at AS 4's provider interface. Assume a reflection attacker is attached to AS 3. It sends packets spoofing P4 to the server located in AS 2 for attacking the victim in AS 4. However, this attack cannot be successfully blocked though AS 4 has deployed inter-domain SAV.

3.2. Underperforming Upstream Checking

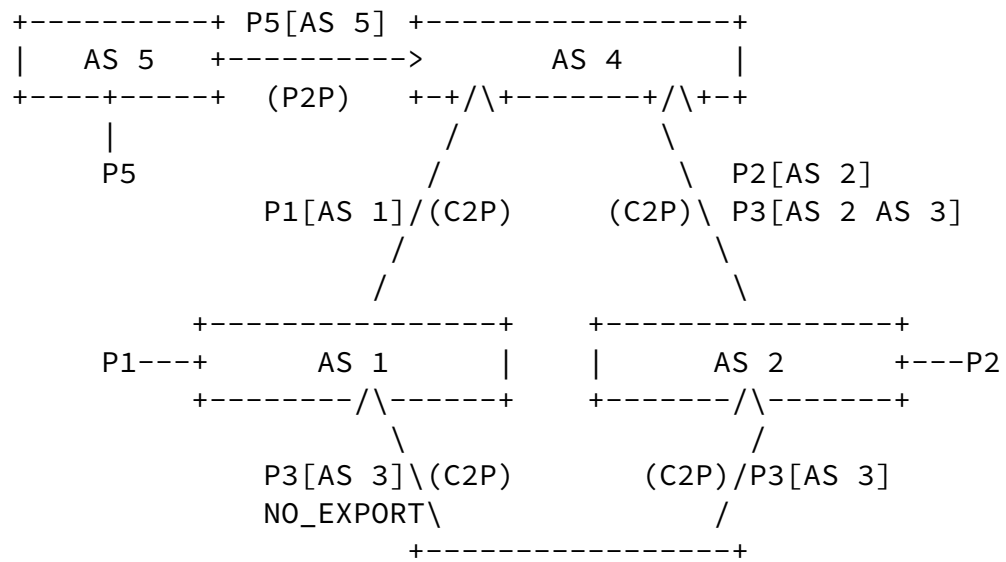
Although, as mentioned above, existing inter-domain SAV mechanisms take a relatively strict SAV for upstream, they may fail in performing proper SAV in some typical cases.

3.2.1. NO_EXPORT in BGP Advertisement

Figure 2 presents an inter-domain scenario where the above inter-domain SAV mechanisms fail. AS 1 and AS 2 are two customer ASes of AS 4. AS 3 is the common customer of AS 1 and AS 2. AS 5 is the lateral peer of AS 4. All arrows in Figure 2 represent BGP advertisements. AS 1 owns prefix P1 and advertises it to AS 4. AS 2 owns prefix P2 and AS 5 owns prefix P5. P2 and P5 are also advertised to AS 4 through BGP. AS 3 owns prefix P3 and advertises it to AS 1 and AS 2, respectively. After receiving the route for prefix P3 from AS 3, AS 2 propagates this route to AS 4. Differently, AS 1 does not propagate the route for prefix P3 to AS 4, since AS 3 adds the NO_EXPORT community attribute in the BGP advertisement destined to AS 1. In the end, AS 4 only learns the route for prefix P3 from AS 2.

If AS 4 runs strict uRPF/FP-uRPF/EFP-uRPF with algorithm A at customer interfaces, packets with source addresses of P3 are required to arrive only from AS 2. When AS 3 sends packets with legitimate source addresses of prefix P3 to AS 4 through AS 1, AS 4 will improperly block these packets.

Besides the NO_EXPORT case above, there are also many route filtering policies that can result in interruption of BGP advertisement and may lead to improper block problems of existing inter-domain SAV mechanisms.



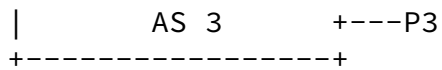


Figure 2: Interrupted BGP advertisement caused by NO_EXPORT

3.2.2. Spoofing within Customer Cone

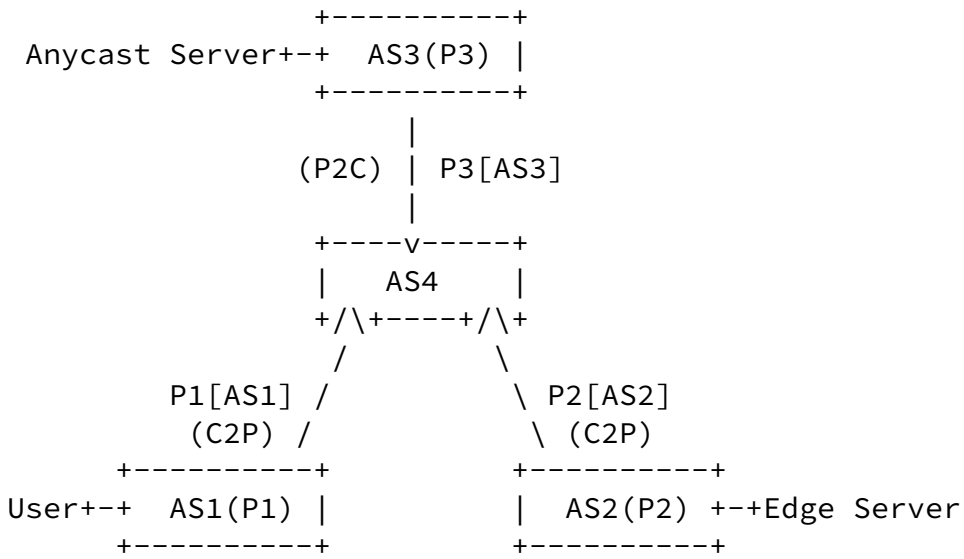
To mitigate the improper block problem, EFP-uRPF with algorithm B is recommended in RFC8704. It allows packets with source addresses of the customer cone to enter from any customer interfaces to avoid potential improper block problems resulted by interrupted BGP advertisement. However, another vulnerability is imported. Although EFP-uRPF with algorithm B can prevent ASes inside the customer cone from using source addresses of ASes outside the customer cone, it sacrifices the directionality of traffic from different customers, which will lead to improper permit problems.

In Figure 2, assume AS 4 implements EFP-uRPF with algorithm B at customer interfaces. Under EFP-uRPF with algorithm B, AS 4 will generate SAV rules with legitimate P1, P2, and P3 at both customer interfaces. When the attacker in AS 1 spoofs source address of AS 2, AS 4 will improperly permit these packets with spoofed source addresses of prefix P2. The same also applies when the attacker in AS 2 forges prefix P1. That is to say, EFP-uRPF algorithm B cannot prevent source address spoofing between ASes of the customer cone.

3.2.3. Direct Server Return (DSR) Scenario

Anycast is a network addressing and routing methodology. An anycast IP address is shared by devices in multiple locations, and incoming requests are routed to the location closest to the sender. Therefore, anycast is widely used in Content Delivery Network (CDN) to improve the quality of service by bringing the content to the user as soon as possible. In practice, anycast IP addresses are usually

announced only from some locations with a lot of connectivity. Upon receiving incoming requests from users, requests are then tunneled to the edge locations where the content is. Subsequently, the edge locations do direct server return (DSR), i.e., directly sending the content to the users. To ensure that DSR works, servers in edge locations must send response packets with anycast IP address as the source address. However, since edge locations never advertise the anycast prefixes through BGP, an intermediate AS with strict uRPF/FP-uRPF/EFP-uRPF may improperly block these response packets.



P3 is the anycast prefix and is only advertised from AS3

Figure 3: A Direct Server Return (DSR) scenario

Figure 3 shows a specific DSR scenario. The anycast IP prefix (i.e., prefix P3) is only advertised from AS 3 through BGP. Assume AS 3 is the provider of AS 4. AS 4 is the provider of AS 1 and AS 2. When users in AS 1 send requests to the anycast destination IP, the forwarding path from users to anycast servers is AS 1 -> AS 4 -> AS 3. Anycast servers in AS 3 receive the requests and then tunnel them to the edge servers in AS 2. Finally, the edge servers send the content to the users with source addresses of prefix P3. The reverse

forwarding path is AS 2 -> AS 4 -> AS 1. Since AS 4 never receives

routing information for prefix P3 from AS 2, strict uRPF/feasible uRPF/EFP-uRPF algorithm A/EFP-uRPF algorithm B at AS 4 will improperly block the response packets from AS 2.

4. Problem Statement

4.1. Limitation in Accuracy

High accuracy, i.e., avoiding improper block problems while trying best to reduce improper permit problems, is the basic and key problem of an SAV mechanism. Existing inter-domain SAV mechanisms have accuracy gaps in some scenarios like routing asymmetry induced by local BGP policies or ACL redirection rules. Particularly, EFP-uRPF takes the RPF list in data-plane, which means the packets from customer interfaces with unknown source prefixes (not appear in the RPF list) will be discarded directly. Improper block issues will arise when legitimate source prefixes are not accurately learned by EFP-uRPF. The root cause is that these mechanisms leverage local RIB table of routers to learn the source addresses and determine the valid incoming interface, which may not match the real data-plane forwarding path from the source. It may mistakenly consider a valid incoming interface as invalid, resulting in improper block problems; or consider an invalid incoming interface as valid, resulting in improper permit problems. Essentially, it is impossible to generate an accurate SAV table solely based on the router's local information due to the existence of asymmetric routes.

4.2. Misaligned Incentive

Existing inter-domain SAV mechanisms pay more attention to upstream (traffic from customer to provider/peer), resulting in weak source address checking of downstream (traffic from provider/peer to customer). The deployed network is still vulnerable to reflection attack, which is considered the most harmful source address spoofing attack, from other networks. Besides, "strict upstream but weak downstream checking" makes the benefits of deploying SAV flow to the rest of the Internet, but not to the deployed network itself. This will harm the incentive of ASes deploying SAV.

5. Requirements

Inter-domain SAVNET focuses on narrowing the technical gaps of existing inter-domain SAV mechanisms. The architecture of inter-domain SAVNET should satisfy the following requirements.

5.1. Accurate Path Discovery

To guarantee the accuracy of SAV, the AS should learn the real data-plane forwarding path from each source. Incomplete path discovery will result in improper block problems (e.g., in asymmetric routing scenarios), while including unused paths will lead to improper permit problems. Some other path discovery mechanisms should be imported as an addition to the method based on RIB.

5.2. All-round Protection

It is desired that downstream are under the same SAV criteria as upstream and that local SAV-enabled AS/cone are also protected well (e.g., protected from reflection attacks). It would be easy to achieve perfect all-round protection supposing SAV is fully deployed, but, unfortunately, it is improbable in the recent future. Even so, efforts are needed to narrow the gaps as possible.

5.3. Incremental Deployment and Incentive

Good incentive is also an essential requirement of inter-domain SAV mechanisms. It would be attractive if the networks deployed with SAV mechanisms are protected from source address spoofing attacks instead of only providing protection to others.

6. Security Considerations

TBD

7. Acknowledgments

TBD

8. Normative References

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[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>.

[RFC5210] Wu, J., Bi, J., Li, X., Ren, G., Xu, K., and M. Williams, "A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience", RFC 5210, DOI 10.17487/RFC5210, June 2008, <https://www.rfc-editor.org/info/rfc5210>.

[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>.

[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>.

Authors' Addresses

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

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn

Lancheng Qin
Tsinghua University
Beijing
China
Email: qlc19@mails.tsinghua.edu.cn

Mingqing Huang

Huawei
Beijing
China
Email: huangmingqing@huawei.com

Nan Geng
Huawei
Beijing
China
Email: gengnan@huawei.com