Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 6, 2022

D. Li
J. Wu
Tsinghua
Y. Gu
Huawei
L. Qin
Tsinghua
T. Lin
H3C

July 5, 2021

Soure Address Validation: Gap Analysis
draft-li-opsec-sav-gap-analysis-02

Abstract

This document identifies scenarios where existing IP spoofing approaches for detection and mitigation don't perform perfectly. Exsiting SAV (source address validation) approaches, either Ingress ACL filtering [RFC2827], unicast Reverse Path Forwarding (uRPF) [RFC3704], Feasible Path uRPF [RFC 3704], or Enhanced Feasible-Path uRPF [RFC8704] has limitations regarding eihter automated implemetation objective or detection accuracy objective (0% false positive and 0% false negative). This document provides the gap analysis of the exsting SAV approaches, and also provides solution discussions.

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 2119 [RFC2119].

Status of This Memo

This Internet-Draft will expire on January 6, 2022.

Copyright Notice

Table of Contents

1. Introduction

1.1. Source Address Validation

The Internet is open to traffic, which means that a sender can generate traffic and send to any receiver in the Internet as long as the address is reachable. Although this openness design improves the scalability of the Internet, it also leaves security risks, e.g., a sender can forge the source address when sending the packets, which is also known as IP spoofing. IP spoofing is constantly used in Denial of Service (DoS) attacks, which seriously compromise network security. DOS attacks using IP spoofing makes it difficult for operators to locate the attacker's actual source address. [RFC6959] identifies different types of DOS attacks with IP spoofing, i.e., single-packet attack, flood-based DoS, poisoning attack, spoof-based

worm/malware propagation, reflective attack, accounting subversion, man-in-the-middle attack, third-party recon, etc.

1.2. Existing SAV Techniques Overview

Source address validation (SAV) verifies the authenticity of the packet's source address to detect and mitigate IP spoofing [RFC2827]. Existing methods, such as Source Address Validation Improvement (SAVI) [RFC7039], unicast Reverse Path Forwarding (uRPF) (i.e., Strict uRPF, Feasible uRPF and Loose uRPF) [RFC3704], as well as Enhanced Feasible-Path Unicast Reverse Path Forwarding (EFP-uRPF) methods [RFC8704] are deployed at different network levels to prevent IP spoofing.

Overall, when evaluating a SAV technique, one should consider the following two perspectives.

1) Precise filtering: Two important indicators for precise filtering. 1) 0% false positive (FP) rate. If legitimate packets are dropped, it can seriously affect the user experience. 2) 0% false negative (FN) rate. If some packets with a forged source address passes, it poses potential security risks.

2) Automatic implementation: In practice, the address space may grow, and routing policies may be dynamically adjusted. SAV solutions that rely entirely on manual configuration are either non-scalable or error-prone.

SAVI, typically performed at the access network, is enforced in switches, where the mapping relationship between an IP address and other "trust anchor" is maintained. A "trust anchor" can be link-layer information (such as MAC address), physical port of a switch to connect a host, etc. It enforces hosts to use legitimate IP source addresses. However, given numerous access networks managed by different operators, it is far from practice for all the access networks to simultaneously deploy SAVI. Therefore, in order to mitigate the security risks raised by source address spoofing, SAV performed in network border routers is also necessary. Although it does not provide the same filtering granualarity as SAVI does, it still helps the tracing of spoofing to a minimized network range.

Ingress ACLs [RFC2827], typically performed at the network border routers, is performed by manually maintaining a traffic filtering access list which contains acceptable source address for each interface. Only packets with a source address encompassed in the access list can be accepted. It strictly specifies the source address space of incoming packets. However, manual-based filtering method is error-prone and face scalability issues.

Strict uRPF, typically performed at the network (IGP areas or ASes) border routers, requires that a data packet can be only accepted when the FIB contains a prefix that encompasses the source address and the corresponding out-interface matches the data incoming interface. It has the advantages of simple operation, easy deployment, and automatic update. However, in case of multihoming, when the data imcoming interface is different from the out-interface, which is also refered to as asymmetric routing of data packets, Strict uRPF exibits FP.

Loose uRPF, sacrificing the directionality of Strict uRPF, only requires that the packet's source IP exists as a FIB entry. Intuitively, Loose uRPF cannot prevent the attacker from forging a source address that already exists in the FIB, which incurs FN detection.

Feasible uRPF (FP-uRPF), typically performed at the network border routers, helps mitigate FP of Strict uRPF in the multihoming scenarios. Instead of installing only the best route into FIB as Strict uRPF does, Feasible uRPF installs all alternative paths into the FIB. It helps reduce FP filtering compared with the Strict uRPF, in the case when multiple paths are learnt from different interfaces. However, it should be noted that Feasible uRPF only works when multiple paths are learnt. There are cases when a device only learns one path but still has packets coming from other valid interfaces. Thus, FP-uRPF performs better than Loose uRPF regarding FP detection, but still doesn't not guarantee 0% FP.

EFP-uRPF, specifically performed at the AS border routers, further improves FP-uRPF in the inter-AS scenario. An ASBR, performing EFP-uRPF, maintains an RPF filtering list on each customer/peer interface. It introduces two algorihtms (i.e., Algorithm A and Algorithm B) regarding different application scenarios. In the case that a customer interface fails to learn any route from a directly connected customer AS, enabling Algorithm A at this customer interface may exibit false postive detection. In this case, Algorithm B can mitigate the FP. However, in case of two customer ASes spoofing each other, Algorithm B exibits FN.

This document specifically identifies two scenarios, where the above mentioned SAV techniques, i.e., Strict uRPF, Loose uRPF, FP-uRPF, and EFP-uRPF, fail to guarantee 0% FP and 0% FN detection.

2. Terminology

IGP: Interior Gateway Protocol

IS-IS: Intermediate System to Intermediate System

BGP: Boarder Gateway Protocol

RIB: Routing Information Base

FIB: Forwarding Information Base

SAV: Source Address Validation

AD: Administrative Domain

3. Problem Statement

3.1. Use Case 1: Inter-AS Multi-homing

Figure 1 illustrates an inter-AS multihoming case.

AS2 is multi-homed to AS1 and AS4. AS2 announces P1/P2 to AS1 through BGP. AS2 doesn't announce any of its routes to AS4 due to policy control. P1/P2 are propagated from AS1 to AS4 through BGP.

AS3 is single-homed to AS4. AS3 announces P3 to AS4 through BGP. AS4 propagates P3 to AS1 through BGP.

Now suppose two data flows coming from AS2 to AS4: Flow 1 with source IP as P1, and Flow 2 with source IP as P3 (IP spoofing). Using existing SAV methods at AS4, Flow 1 is supposed to be passed, while Flow 2 is supposed to be dropped.

- Loose uRPF: works for Flow 1, but fails for Flow 2.

- Strict uRPF: works for Flow 2, but fails for Flow 1 (the incoming interface does not match P1/P2's out-interface).

- FP-uRFP: works for Flow 2, but fails for Flow 1 (no feasible path for P1/P2 other than the best route exists).

- EFP-uRPF: works for Flow 1, but fails for Flow 2 using Algorithm B. Works for Flow 2, but fails for Flow 1 when using Algorithm A.

```
                          P1[AS1 AS2]
                          P2[AS1 AS2]
      +---------------+      (C2P)       +---------------+
      |               +------------------>               |
      |      AS1      |                  |      AS4      |
      |               <------------------+               |
      +----+/\+-------+   P3[AS4 AS3]    ++/\+-----+/\+--+
             \               (P2C)         /         \
              \                           /           \
            P1[AS2]              [no prefix adv]     P3[AS3]
            P2[AS2]                     /               \
           (C2P) \                     / (C2P)           \ (C2P)
                  \                   /                   \
                   \                 /                     \
                +---------------------+         +---------------+
                |                     |         |               |
                |    AS2(customer)    |         | AS3(customer) |
                |                     |         |               |
                +---------------------+         +---------------+
              P1,P2(prefixes originated)       P3(prefix originated)
```

Figure 1: Asymmetric data flow in the Inter-AS scenario

3.2. Use Case 2: Intra-AS Multi-homing

Figure 2 illustrates an intra-AS multihoming case. To facilitate management, one AS can be divided into several administrative domains (ADs) and managed by different inner groups. In Figure 2, AD1 is the upper level compared to AD2 and AD3, meaning that AD2 or AD3 needs to connect through AD1 for external reachability (i.e., networks outside AD1). For example, AD1 is the backbone of one national education network, while AD2 and AD3 are the campus networks of the two universities.

Router 1 is multi-homed to Router 2 and Router 3. No dynamic routing protocol set up between Router 1 and Router 2, as well as between Router 1 and Router 3. In AD2, static routes to outside AD2 are configured on Router 1 with Router 3 as the next hop. In AD1, static route to P1 is configured on Router 2 and static route to P2 is configured on Router 3, due to traffic control purpose. Router 2 and Router 3 are connected with each other using ISIS or OSPF.

Router 5 is single-homed to Router 3. In AD3, static routes to outside AD3 are configured on Router 5 with Router 3 as the next hop. In AD1,static route to P3 is configured on Router 3 with Router 5 as the next hop.

Now suppose two data flows coming from Router 1 to Router 3: Flow 1 with source IP as P1, and Flow 2 with source IP as P3 (IP spoofing). Using existing SAV methods at Router 3, Flow 1 is supposed to be passed, while Flow 2 is supposed to be dropped.

- Loose uRPF: works for Flow 1, but fails for Flow 2.

- Strict uRPF: works for Flow 2, but fails for Flow 1 (the incoming interface does not match P1's out-interface).

- FP-uRFP: works for Flow 2, but fails for Flow 1 (no feasible path for P1 other than the best route exists).

- EFP-uRPF: does not apply at the intra-AS case.

```
+----------------------------------------------------------------------+
|    AS                                                                |
|                 +--------------------------------+                   |
|                 | AD1     +------------+         |                   |
|                 |         |  Router 4  |         |                   |
|                 |         +-/\------/\-+         |                   |
|  Router 2       |           /        \           |    Router 3       |
|  Static RIB:    |          /          \          |    Static RIB:    |
|  Prefix: P1     | +--------+   [P1]   +--------+ |    Prefix: P2     |
|  NH: Router 1   | |        +---------->        | |    NH: Router 1   |
|                 | |Router 2|          |Router 3| |    Prefix: P3     |
|  IGP RIB:       | |        <----------+        | |    NH: Router 5   |
|  Prefix: P2     | +--------+  [P2,P3] +--------+ |                   |
|  NH: Router 3   +---/\-----------------/\----/\--+    IGP RIB:       |
|  Prefix: P3          \                 /      \       Prefix: P1     |
|  NH: Router 3         \               /        \      NH: Router 2   |
|                        \             /          \                    |
|               [no prefix adv]  [no prefix adv] [no prefix adv]       |
|                          \         /              \                  |
|                   +-------\-------/----+    +------\---------+       |
|                   |AD2  +----------+   |    |AD3  +--------+ |       |
|                   |     | Router 1 |   |    |     |Router 5| |       |
|                   |     +----------+   |    |     +--------+ |       |
|                   |        P1,P2       |    |      P3        |       |
|                   +--------------------+    +----------------+       |
|                 P1,P2(prefixes originated)  P3(prefix originated)    |
|                                                                      |
+----------------------------------------------------------------------+
```

Figure 2: Asymmetric data flow in the Intra-AS scenario

4. Solution Discussions

Both EFP-uRPF and FP-uRPF try to achieve a balance between flexibility (Loose uRPF) and directionality (Strict uRPF).

In the inter-AS multi-homing scenario, EFP-uRPF further improves FR-uRPF's directionality. The key improvement of EFP-uRPF is that it synchronizes certain information between interfaces that share the same RPF filtering list, so as to construct an RPF list as comprehensive as possible, although [RFC8704] does not explicitly specify how the information is synchronized, e.g., what information, in which format and in which way. In addition, the construction of RPF lists can be further augmented with data from Route Origin Authorization (ROA) [RFC6482], as well as Internet Routing Registry (IRR) data. In fact, the global availability of ROA and IRR databeses provides a secondary information synchronization approach. However, EFP-uRPF still fails to achieve 0% FN and 0% FP in case of Figure 1. Further infomration synchronization between interfaces might provide further improvement.

The above description works similarly for the intra-AS scenario. Information synchronization is also required in order to achieve higher filtering accuracy.

5. Security Considerations

TBD

6. Contributors

TBD

7. Acknowledgments

TBD

8. Normative References

[I-D.brockners-inband-oam-requirements]
Brockners, F., Bhandari, S., Dara, S., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mozes, D., Mizrahi, T., <>, P. L., and R. Chang, "Requirements for In-situ OAM", draft-brockners-inband-oam-requirements-03 (work in progress), March 2017.

[I-D.ietf-grow-bmp-adj-rib-out]
Evens, T., Bayraktar, S., Lucente, P., Mi, P., and S. Zhuang, "Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)", draft-ietf-grow-bmp-adj-rib-out-07 (work in progress), August 2019.

[I-D.ietf-grow-bmp-local-rib]
Evens, T., Bayraktar, S., Bhardwaj, M., and P. Lucente, "Support for Local RIB in BGP Monitoring Protocol (BMP)", draft-ietf-grow-bmp-local-rib-11 (work in progress), April 2021.

[I-D.ietf-netconf-yang-push]
Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", draft-ietf-netconf-yang-push-25 (work in progress), May 2019.

[I-D.openconfig-rtgwg-gnmi-spec]
Shakir, R., Shaikh, A., Borman, P., Hines, M., Lebsack, C., and C. Morrow, "gRPC Network Management Interface (gNMI)", draft-openconfig-rtgwg-gnmi-spec-01 (work in progress), March 2018.

[I-D.song-ntf]
Song, H., Zhou, T., Li, Z., Fioccola, G., Li, Z., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Toward a Network Telemetry Framework", draft-song-ntf-02 (work in progress), July 2018.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)", RFC 1157, DOI 10.17487/RFC1157, May 1990, <https://www.rfc-editor.org/info/rfc1157>.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, DOI 10.17487/RFC1191, November 1990, <https://www.rfc-editor.org/info/rfc1191>.

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, DOI 10.17487/RFC1195, December 1990, <https://www.rfc-editor.org/info/rfc1195>.

[RFC1213] McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", STD 17, RFC 1213, DOI 10.17487/RFC1213, March 1991, <https://www.rfc-editor.org/info/rfc1213>.

[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>.

[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>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[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>.

[RFC3719] Parker, J., Ed., "Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)", RFC 3719, DOI 10.17487/RFC3719, February 2004, <https://www.rfc-editor.org/info/rfc3719>.

[RFC3988] Black, B. and K. Kompella, "Maximum Transmission Unit Signalling Extensions for the Label Distribution Protocol", RFC 3988, DOI 10.17487/RFC3988, January 2005, <https://www.rfc-editor.org/info/rfc3988>.

[RFC6232] Wei, F., Qin, Y., Li, Z., Li, T., and J. Dong, "Purge Originator Identification TLV for IS-IS", RFC 6232, DOI 10.17487/RFC6232, May 2011, <https://www.rfc-editor.org/info/rfc6232>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <https://www.rfc-editor.org/info/rfc6959>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <https://www.rfc-editor.org/info/rfc7039>.

[RFC7752] Gredler, H., Ed., Medved, J., Previdi, S., Farrel, A., and S. Ray, "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP", RFC 7752, DOI 10.17487/RFC7752, March 2016, <https://www.rfc-editor.org/info/rfc7752>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/info/rfc7854>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/info/rfc8210>.

[RFC8231] Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE", RFC 8231, DOI 10.17487/RFC8231, September 2017, <https://www.rfc-editor.org/info/rfc8231>.

[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

Dan Li
Tsinghua
Beijing
China

Email: tolidan@tsinghua.edu.cn

Jianping Wu
Tsinghua
Beijing
China

Email: jianping@cernet.edu.cn

Yunan Gu
Huawei
Beijing
China

Email: guyunan@huawei.com

Lancheng Qin
Tsinghua
Beijing
China

Email: qlc19@mails.tsinghua.edu.cn

Tao Lin
H3C
Beijing
China

Email: lintao@h3c.com