SAVI J. Bi
Internet-Draft B. Liu
Intended status: Informational Tsinghua Univ.
Expires: November 25, 2013 May 24, 2013

Problem Statement of SAVI Beyond the First Hop
draft-bi-savi-problem-05

Abstract

IETF Source Address Validation Improvements (SAVI) working group is chartered for source address validation within the first hop from the end hosts, i.e. preventing a node from spoofing the IP source address of another node in the same IP link. However, since SAVI requires the edge routers or switches to be upgraded, the deployment of SAVI will need a long time. During this transition period, some source address validation techniques beyond the first hop (SAVI-BF) may be needed to complement SAVI and protect the networks from spoofing based attacks. In this document, we first propose three desired features of the SAVI-BF techniques. Then we analyze the problems of the current SAVI-BF technique, ingress filtering. Finally, we discuss the directions that we can explore to improve SAVI-BF.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

IETF Source Address Validation Improvements (SAVI) working group is chartered for source address validation within the first hop from the end hosts, i.e. preventing a node from spoofing the IP source address of another node in the same IP link. However, since SAVI requires the edge routers or switches to be upgraded, the deployment of SAVI will need a long time. During this transition period, some source address validation techniques beyond the first hop (SAVI-BF) may be needed to complement SAVI, so as to protect the networks from spoofing based attacks, which are prevalent DDoS attacks on the current Internet [Ground-Truth] [ARBOR-2010] [ARBOR-2009] [NANOG-Helpless].

In this document, we first propose three desired features of SAVI-BF techniques. The first desired feature is high deployment incentives, i.e. by deploying a technique, an ISP should significantly increase its ability to protect its network from spoofing based attacks. The second one is low operational risks. If a technique may improperly drop legitimate packets (so called false positive), it introduces new risks into the network operation and management. It is desired that the false positive (FP) is as low as possible. The third one low cost. It is desired that the technique requires minimum deployment investment and operational cost.

We evaluate ingress filtering [BCP38] [BCP84], the best current practice in spoofing prevention, against these three features. Recent measurement shows that, the deployment of ingress filtering has not been improved over four years because the ISPs do not have incentive to deploy it [Efficacy], and sophisticated attackers exploit the spoofable networks to launch attacks. We discuss the reasons why ingress filtering is still insufficiently applied by the ISPs despite that it has long been available in modern routers.

Finally, we discuss the directions that we can explore to improve SAVI-BF. We briefly survey two categories of SAVI-BF proposals, the path based techniques and the end-to-end based techniques. We discuss their requirements, advantages and disadvantages.

2. Desired Features of SAVI-BF Techniques

2.1. High Deployment Incentives

To motivate an ISP to deploy a technique, it is desirable that the technique can generate additional benefit for the ISP. In terms of a SAVI-BF technique, it should provide the ISP with additional protection from spoofing based attacks. Specifically, it should

significantly decrease the volume of the spoofing based attacks targeting the ISP, or the number of networks where these attacks can be successfully launched, or the number of source addresses or destination addresses that can be used in these attacks.

2.2. Low Operational Risks

If a technique may improperly drop legitimate packets, so called false positives (FP), it introduces new operational risks. Apparently, it is desired that the FP is as low as possible. The higher the FP is, the more limited its application scope is. For example, if the attack is not very severe, the network administrator won't apply a technique with high FP, since its operation risks may even surpass the loss caused by the attack.

2.3. Low Cost

It is desired that the technique requires minimum investment on the device and system upgrading. It should also adapt to network dynamics rather than require manual intervention, which is costly, slow, and often the source of errors (misconfiguration).

3. Problems of Ingress Filtering

Ingress filtering is the best current practice for SAVI-BF. Ingress filtering was proposed in 2000 [BCP38] , and updated in 2004 [BCP84]. Ingress access lists (IALs) and unicast reverse path forwarding (uRPF) are two general ways to implement ingress filtering. An IAL is a filter that checks the source address of every packet received on a network interface against a list of acceptable prefixes, dropping any packet that does not match the filter. IALs are typically maintained manually. Upon network dynamics (topology change or routing change), the IALs should be updated accordingly to avoid dropping legitimate packets. uRPF is an automated tool which can adapt with the network dynamics. On the receipt of a packet, uRPF checks its source address against the forwarding table or routing table for validation. uRPF has four variants, strict RPF, feasible RPF, loose RPF and loose RPF ignoring default routes. Readers are referred to [BCP84] for the details of these variants.

Today, many modern routers are capable of ingress filtering. Many network administrators have turned on uRPF on their routers or been actively maintaining IALs to filter spoofing traffic. The fraction of networks where spoofing is possible is significantly limited [MIT-Spoofer]. However, as shown by the recent measurement, the deployment of ingress filtering has not been improved over four years. Sophisticated attackers can still exploit the networks where

spoofing is possible to launch spoofing based attacks, and IP spoofing remains a viable attack vector on the current Internet [Efficacy].

In this section, we evaluate ingress filtering against the desired features, and analyze the reasons why ingress filtering is not sufficiently deployed, and why its deployment has not been improved over years. We classify the five variants of ingress filtering (IAL and four variants of uRPF) into three categories according to their technical similarities, i.e. IALs, strict/feasible RPF, and loose RPF* (including loose RPF and loose RPF ignoring default routes). The evaluation results are summarized in Table 1, which we will explain in detail in the following subsections.

Techniques	Incentive	Risk	Cost
IAL	low	low	low
-			
Strict/feasible RPF	high	high	low
-			
Loose RPF*	low	low	low

Table 1: Evaluation of Ingress Filtering

3.1. IAL

In practice, IAL is typically applied near the source end, i.e. near the hosts who originate the traffic. When applied at the destination end or intermediate nodes, the incoming direction of a source prefix is hard to determine. Especially when the routing is dynamic, manually maintaining IALs is almost impossible. As a result, deploying IAL (at the source end) is all about "being a good Internet citizen", but it provides very little self-protection to the ISPs [NANOG-Incentive]. Thus IAL has low deployment incentives. If applied in relatively stable networks near the source end, manual configuration can be feasible, and won't cause high FP. Thus the operational cost is also low. IALs can be implemented using access control list (ACL), which is a common function in the modern routers. This lowers the cost of IAL.

3.2. Strict/feasible RPF

Strict and feasible RPF can adapt themselves to the routing dynamics and determine the incoming directions of source prefixes automatically. They are more effective than IAL in detecting and filtering spoofing traffic, and thus provide higher deployment

incentives to the ISPs. However, they often drop legitimate packets under routing asymmetry, which is very prevalent with the existence of local routing policies, multi-homing and traffic engineering. This makes strict and feasible very risky [NANOG-Risk], and hence the operation needs to be very careful. Feasible RPF has lower FP than strict RPF, since it can apply multiple interfaces as acceptable incoming directions for a source prefix. But feasible RPF cannot avoid all FP in practice, since currently there is no practical way to generate and configure all possible incoming directions in the routers. For example, in a link-state routing environment (IS-IS or OSPF), equal-cost multi-path (ECMP) [ECMP] is often used to generate the multiple acceptable incoming directions. However, in practice, there can be many (tens of) ECMPs for a prefix, but the implementation of a router can only store several (e.g. 4 or 8) of them. Thus the ECMPs for the prefix installed in the forwarding table may be different in different routers, which eventually causes the FP of feasible RPF. And in BGP, the directions where BGP announcements for a source address prefix have been received can be considered as acceptable incoming directions [IDPF]. However, an ISP may choose not to announce a prefix via a path but still send traffic through it due to its local routing policy. In this case, feasible RPF also causes FP. The basic function of strict and feasible RPF is supported in most modern routers. So deploying them doesn't require investment on upgrading devices.

3.3. Loose RPF*

Instead of validating the incoming direction of a source address, loose RPF* only checks the existence of the source address in the forwarding table. Loose RPF* is only useful for filtering Martian addresses and unroutable addresses. However, sophisticated attackers can evade loose RPF* checking by simply using routable source addresses. Thus the incentive to deploy loose RPF is low. On the other hand, its operational risk is also low. Loose RPF* is also available in most modern routers, making it cheap to deploy.

There are other reasons why the deployment of ingress filtering hasn't been improved in four years. First, although most modern routers are capable of ingress filtering, some legacy routers are incapable [NANOG-Equipment]. Hence, even at the locations where no risk exists (e.g. stub or single-homed networks), ingress filtering may not be applied. Another reason is called inertia. Since ingress filtering is not enabled on routers by default, some network administrators just won't bother to turn it on [NANOG-PowerOfDefaults].

4. Discussion

In this section, we discuss the directions that we can explore to improve SAVI-BF. We briefly survey two categories of SAVI-BF proposals, the path based techniques and the end-to-end based techniques. We discuss their requirements, advantages and disadvantages. We only focus on the techniques that are implemented on the routers. The techniques implemented on end hosts, such as [IPSec], [HCF] and [IP-Puzzles], are not covered here.

4.1. Path based Techniques

The path based techniques essentially require that a router R knows the forwarding paths that each source prefix S uses toward its destinations, and subsequently knows the incoming directions/ interfaces of S. Sometimes, this information is available to R. For example, in a pure link-state routing protocol environment (e.g. IS-IS, OSPF), all nodes have the same view of the network. Thus, R can compute the paths from S to all destinations, and then infer the incoming directions of S. One exception is that, when there are multiple equally best paths, R may not determine which one S will use. On the other hand, if a distance-vector (e.g. RIP) or a path-vector (BGP) routing protocol is used, it is even harder for R to determine the paths of S, since the sufficient routing information is missed. [SAVE] and [IDPF] are tow proposals which validate source addresses by inferring their forwarding paths.

4.2. End-to-end based Techniques

There are, however, other proposals that don't rely on path information. We call them end-to-end based techniques. For example, [SPM] associates each source prefix (indeed, source AS number) with a key. S, an SPM-enabled AS, will tag the key into outbound packets toward R at its border routers. And R verifies the keys of the inbound packets whose source addresses belong to S at its border routers. The routers will drop a packet if the key is incorrect. Thus, R manages to validate the source addresses of S without knowing its forwarding paths. The end-to-end based the techniques typically need the cooperation between the source and the verification nodes, and require particular tags be carried in the data packets. Further more, even the end-to-end based techniques require to distinguish inbound traffic and outbound traffic, which is not completely path-independent.

4.3. Non-technical Proposals

There are also proposals which formulate source address validation as an economic problem [FaaS], or suggest that laws and governance

should be enforced. These directions, however, may be out of the scope of IETF.

5. Acknowledgment

The authors would like to thank Fred Baker and Joel M. Halpern for their comments.

This document was generated using the xml2rfc tool.

6. Informative References

[ARBOR-2009]
McPherson, D., Dobbins, R., Hollyman, M., Labovitz, C., and J. Nazario, "Network Infrastructure Security Report", February 2009.

[ARBOR-2010]
Dobbins, R. and C. Morales, "Network Infrastructure Security Report", February 2010.

[BCP38] Paul, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, BCP 38, May 2000.

[BCP84] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", RFC 3704, BCP 84, March 2004.

[ECMP] Thaler, D. and C. Hopps, "Multipath Issues in Unicast and Multicast Next-Hop Selection", RFC 2991, November 2000.

[Efficacy]
Beverly, R., Berger, A., Hyun, Y., and k. claffy, "Understanding the Efficacy of Deployed Internet Source Address Validation Filtering", August 2009.

[FaaS] Liu, B., Bi, J., and X. Yang, "FaaS: Filtering IP Spoofing Traffic as a Service", 2012.

[Ground-Truth]
Labovitz, C., "Botnets, DDoS and Ground-Truth", October 2010.

[HCF] Jin, C., Wang, H., and K. Shin, "Hop-count filtering: an effective defense against spoofed DDoS traffic", 2003.

[IDPF] Duan, Z., Yuan, X., and J. Ch, "Controlling IP Spoofing Through Inter-Domain Packet Filters", 2008.

[IP-Puzzles]
Feng, W., Feng, W., and A. Luu, "The Design and Implementation of Network Puzzles", 2005.

[IPSec] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[MIT-Spoofer]
Beverly, R., "Spoofer Project", January 2012, <http://spoofer.csail.mit.edu/>.

[NANOG-Equipment]
Bicknell, L., "BCP38 Deployment", March 2012, <http://mailman.nanog.org/pipermail/nanog/2012-March/047139.html>.

[NANOG-Helpless]
Bulk, F., "Are we really this helpless? (Re: isprime DOS in progress)", January 2009, <http://mailman.nanog.org/pipermail/nanog/2009-January/006996.html>.

[NANOG-Incentive]
Bicknell, L., "BCP38 Deployment", March 2012, <http://mailman.nanog.org/pipermail/nanog/2012-March/047134.html>.

[NANOG-PowerOfDefaults]
Donelan, S., "BCP38 Deployment", March 2012, <http://mailman.nanog.org/pipermail/nanog/2012-March/047147.html>.

[NANOG-Risk]
Gilmore, P., "BCP38 Deployment", March 2012, <http://mailman.nanog.org/pipermail/nanog/2012-March/047087.html>.

[SAVE] Li, J., Mirkovic, J., Wang, M., Reiher, P., and L. Zhang, "SAVE: Source Address Validity Enforcement Protocol", 2002.

[SPM] Anat, A. and H. Hanoch, "Spoofing Prevention Method", March 2005.

Authors' Addresses

Jun Bi
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China

Email: junbi@tsinghua.edu.cn

Bingyang Liu
Tsinghua University
Computer Science, Tsinghua University
Beijing 100084
China

Email: liuby@netarchlab.tsinghua.edu.cn