Internet Engineering Task Force (IETF)
Request for Comments: 6959
Category: Informational
ISSN: 2070-1721

D. McPherson
VeriSign, Inc.
F. Baker
Cisco Systems
J. Halpern
Ericsson

May 2013

Source Address Validation Improvement (SAVI) Threat Scope

Abstract

The Source Address Validation Improvement (SAVI) effort aims to complement ingress filtering with finer-grained, standardized IP source address validation. This document describes threats enabled by IP source address spoofing both in the global and finer-grained context, describes currently available solutions and challenges, and provides a starting point analysis for finer-grained (host granularity) anti-spoofing work.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6959.

Copyright Notice

Table of Contents

1. Overview

The Internet Protocol, specifically IPv4 [RFC0791] and IPv6 [RFC2460], employs a connectionless hop-by-hop packet forwarding paradigm. A host connected to an IP network that wishes to communicate with another host on the network generates an IP packet with source and destination IP addressing information, among other options.

At the IP network layer, or Internet layer, there is typically no required transactional state when communicating with other hosts on the network. In particular, the network does not track any state about the hosts using the network. This is normally a benefit. However, as a consequence of this, hosts generating packets for transmission have the opportunity to spoof (forge) the source address of packets that they transmit, as the network does not have any way to tell that some of the information is false.

Source address validation is necessary in order to detect and reject spoofed IP packets in the network, and contributes to the overall security of IP networks. This document deals with the subset of such validation done by the network based on observed traffic and policy. Such source address validation techniques enable detection and rejection of many spoofed packets, and also implicitly provide some assurances that the source address in an IP packet is legitimately assigned to the system that generated the packet.

Solutions such as those described in BCP 38 [RFC2827] provide guidelines for one such technique for network ingress filtering. However, if these techniques are not implemented at the ingress point of the IP network, then the validity of the source address cannot be positively ascertained. Furthermore, BCP 38 only implies source address validation at the Internet layer and is most often implemented on IP subnetwork address boundaries. One of the difficulties in encouraging the deployment of BCP 38 is that there is relatively little benefit until it is very widely deployed, which is not yet the case.

Hence, in order to try to get better behavior, it is helpful to look for an application like that described in BCP 38, but one that can be applied locally and give locally beneficial results. The local benefit would provide a reason for the site to deploy, while moving the Internet as a whole towards an environment where BCP 38 is widely effected. SAVI is aimed at providing more specific protection locally, with the benefit of better local behavior and, in conjunction with appropriate logging, better local traceability, while also providing better compliance with the cases dealt with by BCP 38.

It should be noted that while BCP 38 directs providers to provide protection from spoofed prefixes, it is clearly desirable for enterprise operators to provide that protection more locally, and with better traceability. This allows the enterprise to be a better Internet participant and to quickly detect and remedy problems when they occur. For example, when an enterprise receives a report of an attack originating within that enterprise, the operational staff desires to be able to track from the IP address sourcing the attack to the particular machine within the enterprise that is the source. This is typically simpler and more reliable than other techniques, such as trying to find the attack in ongoing outbound traffic. To do this, the enterprise needs usable address assignment and usage information (appropriate logging), as well as accurate information (SAVI), to determine that no other machine could have been using that address.

Also, there is a possibility that in a LAN environment where multiple hosts share a single LAN or IP port on a switch or router, one of those hosts may spoof the source addresses of other hosts within the local subnet. Understanding these threats and the relevant topologies in which they’re introduced is critical when assessing the threats that exist with source address spoofing.

This document provides additional details regarding spoof-based threat vectors and discusses implications of various network topologies.

2. Glossary of Terms

The following acronyms and terms are used throughout this memo.

Binding Anchor: The relationship used by a device performing source address enforcement to perform the validation and enforcement. Examples in different situations include Layer 2 addresses or physical ports.

BGP: The Border Gateway Protocol, used to manage routing policy between large networks.

CPE Router: Customer Premises Equipment router. The router on the customer premises, whether owned by the customer or the provider. Also called the Customer Edge, or CE, router.

IP Address: An Internet Protocol address, whether IPv4 or IPv6.

ISP: Internet Service Provider. Any person or company that delivers Internet service to another.

MAC Address: An Ethernet address or comparable IEEE 802 series address.

NNI Router: Network-to-Network Interface router. This router interface faces a similar system operated by another ISP or other large network.

PE Router: Provider Edge router. This router faces a customer of an ISP.

Spoofing: The act of sending a datagram header whose contents at the link layer or network layer do not match the network policies and activities on address assignment or claiming. Generally, this corresponds to sending messages with source network or link-layer information that is assigned to or currently properly claimed by some other devices in the network.

TCP: The Transmission Control Protocol, used on end systems to manage data exchange.

uRPF: Unicast Reverse Path Forwarding. A procedure in which the route table, which is usually used to look up destination addresses and route towards them, is used to look up the source address and ensure that one is routing away from it. When this test fails, the event may be logged, and the traffic is commonly dropped.

3. Spoof-Based Attack Vectors

Spoofing is employed on the Internet for a number of reasons, most of which are in some manner associated with malicious or otherwise nefarious activities. In general, two classes of spoof-based attack vectors exist: blind attacks and non-blind attacks. The following sections provide some information on blind and non-blind attacks; these sections also include information on attacks where the spoofing is primarily intended to interfere with tracing the attacks, as well as attacks where spoofing the source address is a necessary component to the damage or interference.

3.1. Blind Attacks

Blind attacks typically occur when an attacker isn’t on the same local area network as a source or target, or when an attacker has no access to the data path between the attack source(s) and the target systems. In this situation, the attacker has no access to the source and target systems.

3.1.1. Single-Packet Attacks

One type of blind attacks, which we’ll refer to here as "single-packet DoS (Denial of Service) attacks", involves an attacking system injecting spoofed information into the network, which either results in a complete crash of the target system, or in some manner poisons some network configuration or other information on a target system so as to impact network or other services.

An example of an attack that can cause a receiving system to crash is what is called a LAND (Local Area Network Denial) attack. A LAND attack would consist of an attacking system sending a packet (e.g., TCP SYN) to a target system that contains both a source and destination address of that target system. The packet would also contain a single value for the port number, used as both the source and destination port number. Certain target systems will then "lock up" when creating connection state associated with the packet or would get stuck in a state where a target system continuously replies to itself. As this is an attack that relies on bugs in the target, it is possible, but by no means certain, that this threat is no longer viable.

Another form of blind attack is a RST (reset) probe ([RFC4953], Section 2.3). The attacker sends a series of packets to a destination that is engaged in a long-lived TCP session. The packets are RST packets, and the attacker uses the known source and destination addresses and port numbers, along with guesses at the sequence number. If he can send a packet close enough to the right value, in theory he can terminate the TCP connection. While there are various steps that have been developed to ameliorate this attack, preventing the spoofing of source addresses completely prevents the attack from occurring.

3.1.2. Flood-Based DoS

Flood-based DoS attack vectors are particularly effective attacks on the Internet today. They usually entail flooding a large number of packets towards a target system, with the hopes of either exhausting connection state on the target system, consuming all packet processing capabilities of the target or intermediate systems, or consuming a great deal of bandwidth available to the target system such that they are essentially inaccessible.

Because these attacks require no reply from the target system and require no legitimate transaction state, attackers often attempt to obfuscate the identity of the systems that are generating the attack traffic by spoofing the source IP address of the attacking traffic flows. Because ingress filtering isn’t applied ubiquitously on the Internet today, spoof-based flooding attack vectors are typically very difficult to trace back. In particular, there may be one or more attacking sources beyond a network’s border, and the attacking sources may or may not be legitimate sources; it’s difficult to determine if the sources are not directly connected to the local routing system. These attacks might be seen as primarily needing to be addressed by BCP 38 deployment, which is not in scope for this document. However, as noted earlier, deployment of SAVI can help remediate lack of BCP 38 deployment, and even when BCP 38 is deployed, SAVI can help provide useful information for responding to such attacks.

Common flood-based DoS attack vectors today include SYN floods, ICMP floods, and IP fragmentation attacks. Attackers may use a single legitimate or spoofed fixed attacking source address, although frequently they cycle through large swaths of address space. As a result, mitigating these attacks on the receiving end with source-based policies is extremely difficult.

If an attacker can inject messages for a protocol that requires control-plane activity, it may be possible to deny network control services at a much lower attack level. While there are various forms of protection deployed against this, they are by no means complete. Attacks that are harder to trace (such as with spoofed addresses) are of course of more concern.

Furthermore, the motivator for spoof-based DoS attacks may actually be to encourage the target to filter explicitly on a given set of source addresses, in order to disrupt access to the target system by legitimate owner(s).

3.1.3. Poisoning Attacks

While poisoning attacks can often be done with single packets, it is also true that a stream of packets can be used to find a window where the target will accept the incorrect information. In general, this can be used to perform broadly the same kinds of poisonings as above, with more versatility.

One important class of poisoning attacks are attacks aimed at poisoning network or DNS cache information, perhaps to simply break a given host’s connection or to enable MITM (Man in the Middle) or other attacks. Network-level attacks that could involve single-packet DoS include Address Resolution Protocol (ARP) cache poisoning and ICMP redirects. The most obvious example, which depends upon falsifying an IP source address, is an on-link attacker poisoning a router’s ARP or Neighbor Discovery (ND) cache. The ability to forge a source address can also be helpful in causing a DNS cache to accept and use incorrect information.

3.1.4. Spoof-Based Worm/Malware Propagation

Self-propagating malware has been observed that spoofs its source address when attempting to propagate to other systems. Presumably, this was done to obfuscate the actual source address of the infected system. This attack is important both in terms of an attack vector that SAVI may help prevent and as a problem that SAVI can help solve by tracing back to find infected systems.

3.1.5. Reflective Attacks

Reflective amplification attacks -- wherein a sender sends a single packet to an intermediary, resulting in the intermediary sending a large number of packets, or much larger packets, to the target -- are a particularly potent DoS attack vector on the Internet today. Many of these attacks rely on using a false source address, so that the amplifier attacks the target by responding to the messages.

DNS is one of the common targets of such attacks. The amplification factor observed for attacks targeting DNS root and other top-level domain name infrastructures in early 2006 was on the order of 72:1 [VRSN-REPORT]. The result was that just 27 attacking sources with 512 kbps of upstream attack bandwidth could generate 1 Gbps of response attack traffic towards a target system.

Smurf attacks employ a similar reflective amplification attack vector, exploiting traditional default IP-subnet-directed broadcast address behaviors that would result in all the active hosts on a given subnet responding to a (spoofed) ICMP echo request from an attacker and generating a large amount of ICMP echo response traffic directed towards a target system. These attacks have been particularly effective in large campus LAN environments where 50K or more hosts might reside on a single subnet.

3.1.6. Accounting Subversion

If an attacker wishes to distribute content or other material in a manner that employs protocols that require only unidirectional flooding and generate no end-to-end transactional state, they may desire to spoof the source IP address of that content in order to avoid detection or accounting functions enabled at the IP layer. While this particular attack has not been observed, it is included here to reflect the range of power that spoofed addresses may have, even without the ability to receive responses.

3.1.7. Other Blind Spoofing Attacks

Other blind spoofing attacks might include spoofing in order to exploit source routing or other policy-based routing implemented in a network. It may also be possible in some environments to use spoofing techniques to perform blind or non-blind attacks on the routers in a site or in the Internet. There are many techniques to mitigate these attacks, but it is well known that there are vulnerabilities in this area.

3.2. Non-blind Attacks

Non-blind attacks often involve mechanisms such as eavesdropping on connections, resetting state so that new connections may be hijacked, and an array of other attack vectors. Perhaps the most common of these attack vectors are known as man-in-the-middle attacks. In this case, we are concerned not with an attacker who can modify a stream, but rather with one who has access to information from the stream and uses that information to launch his own attacks.

3.2.1. Man in the Middle (MITM)

Connection hijacking is one of the more common man-in-the-middle attack vectors. In order to hijack a connection, an attacker usually needs to be in the forwarding path and oftentimes employs TCP RST or other attacks in order to reset a transaction. The attacker may have already compromised a system that’s in the forwarding path, or they may wish to insert themselves in the forwarding path.

For example, an attacker with access to a host on a LAN segment may wish to redirect all the traffic on the local segment destined for a default gateway address (or all addresses) to itself in order to perform man-in-the-middle attacks. In order to accomplish this in IPv4, the attacker might transmit gratuitous ARP [RFC0826] messages or ARP replies to the Ethernet broadcast address ff:ff:ff:ff:ff:ff, notifying all the hosts on the segment that the IP address(es) of the target(s) now maps to its own Layer 2 address. The source IP address in this case is spoofed. Similar vulnerabilities exist in the IPv6 ND protocol [RFC4861], although the multicast requirements of the IPv6 ND protocol make this harder to perform with the same generality.

3.2.2. Third-Party Recon

Another example of a non-blind attack is third-party reconnaissance. The use of spoofed addresses, while not necessary for this, can often provide additional information and helps mask the traceability of the activity. The attack involves sending packets towards a given target system and observing either target or intermediate system responses. For example, if an attacker were to source spoof TCP SYN packets towards a target system from a large set of source addresses and observe responses from that target system or some intermediate firewall or other middlebox, they would be able to identify what IP-layer filtering policies may be in place to protect that system.

3.2.3. Other Non-blind Spoofing Attacks

There are presumably many other attacks that can be performed based on the ability to spoof source addresses while seeing the target. Among other attacks, if there are multiple routers on-link with hosts, a host may be able to cause problems for the routing system by replaying modified or unmodified routing packets as if they came from another router.

4. Current Anti-spoofing Solutions

The goal of this work is to reduce datagrams with spoofed IP addresses from the Internet. This can be aided by identifying and dropping datagrams whose source address binding is incompatible with the Internet topology and learned information. This can be done at sites where the relationship between the source address and topology and binding information can be checked. For example, with these bindings, in many networks Internet devices can confirm that:

- The IP source address is appropriate for the lower-layer address (they both identify the same system).

- The IP source address is explicitly identified as appropriate for the physical topology; for example, the source address is appropriate for the Layer 2 switch port through which the datagram was received.

- The prefix to which the IP source address belongs is appropriate for the part of the network topology from which the IP datagram was received (while the individual system may be unknown, it is reasonable to believe that the system is located in that part of the network).

In general, this involves two kinds of inspection. The primary action is checking the source IP address in the IP header of IP packets. In order to support such checking, the claimed or assigned IP addresses in messages concerned with such claims or assignments (IP ARP Requests and Responses, DHCP Replies, IPv6 ND Duplicate Address Detection (DAD) messages, etc.) must also be examined and, where appropriate, verified. SAVI is not concerned with verifying IP addresses in the contents of arbitrary higher-level protocol messages.

Filtering points farther away from the source of the datagram can make decreasingly authoritative assertions about the validity of the source address in the datagram. Nonetheless, there is value in dropping traffic that is clearly inappropriate and in maintaining knowledge of the level of trust one can place in an address.

```
             Edge Network 1           CPE-ISP _.------------.
           _.----------------.         Ingress/   ISP A       `--.
      ,--''                  `---.       ,'                       `.
    ,'  +----+  +------+  +------+ `.   /  +------+       +------+  \\
   (    |Host+--+Switch+--+ CPE  +---)-(---+  PE  +- - - -+ NNI  |   )
    `.  +----+  +------+  |Router| ,'   \\ |Router|       |Router|  /
      `---. Host-neighbor +------+'      `.+------+       +--+---+,'
           `----------------''             '--.             |_.-'
                                               `------------'|
                                                             |
             Edge Network 2                 ISP-ISP Ingress |
           _.----------------.                 _.----------.|
      ,--''                  `---.         ,-''             |--.
    ,'  +----+  +------+  +------+ `.     ,+------+       +--+---+.
   (    |Host+--+Switch+--+ CPE  +---)---+-+  PE  +- - - -+ NNI  | \\
    `.  +----+  +------+  |Router| ,'   (  |Router|       |Router|  )
      `---.               +------+'      \\+------+       +------+ /
           `----------------''            `.                     ,'
                                            '--.   ISP B     _.-'
                                                `----------''
```

Figure 1: Points Where an Address Can Be Validated

Figure 1 illustrates five related paths where a source address can be validated:

- o Host to switch, including host to host via the switch
- o Host to enterprise CPE router
- o Enterprise CPE router to ISP edge PE router, and the reverse
- o ISP NNI router to ISP NNI router

In general, datagrams with spoofed IP addresses can be detected and discarded by devices that have an authoritative mapping between IP addresses and the network topology. For example, a device that has an authoritative table between link-layer and IP addresses on a link can discard any datagrams in which the IP address is not associated with the link-layer address in the datagram. The degree of confidence in the source address depends on where the spoofing detection is performed, as well as the prefix aggregation in place between the spoofing detection and the source of the datagram.

4.1. Topological Locations for Enforcement

There are a number of kinds of places, which one might call topological locations, where solutions may or should be deployed. As can be seen in the details below, as the point of enforcement moves away from a single cable attached directly to the host being validated, additional complications arise. It is likely that fully addressing many of these cases may require additional coordination mechanisms across the device that covers the disparate paths.

4.1.1. Host to Link-Layer Neighbor via Switch

The first point at which a datagram with a spoofed address can be detected is on the link to which the source of the datagram is connected. At this point in the network, the source link-layer and IP addresses are both available and can be validated against each other, and potentially against the physical port being used. A datagram in which the IP source address does not match the corresponding link-layer address can be discarded. Of course, the trust in the filtering depends on the trust in the method through which the mappings are developed. This mechanism can be applied by a first-hop router, or switch on the link. The first-hop switch has the most precise information for this.

On a truly shared medium link, such as classic Ethernet, the best that can be done is to validate the link-layer and IP addresses against the mappings. When the link is not shared, such as when the hosts are connected through a switch, the source host can be identified precisely based on the port through which the datagram is received or the Layer 2 address if it is known to the switch. Port identification prevents transmission of malicious datagrams whose link-layer and IP addresses are both spoofed to mimic another host.

Other kinds of links may fall at different places in this spectrum, with some wireless links having easier ways of identifying individual devices than others, for example.

4.1.2. Upstream Switches

In many topologies, there can be additional switches between the host-attached switch and the first router in the network. In these cases, additional issues can arise that affect SAVI operations. If the bridging topologies that connect the switches change, or if the Link Aggregation Control Protocol (LACP) [IEEE802.1AX], the Virtual Router Redundancy Protocol (VRRP), or link management operations change the links that are used to deliver traffic, the switch may need to move the SAVI state to a different port, or the state may need to be moved or reestablished on a different switch.

4.1.3. Upstream Routers

Beyond the first-hop router, subsequent routers may additionally filter traffic from downstream networks. Because these routers do not have access to the link-layer address of the device from which the datagram was sent, they are limited to confirming that the source IP address is within a prefix that is appropriate for a downstream router from which the datagram was received.

Options include the use of simple access lists or the use of Unicast Reverse Path Forwarding (uRPF). Access lists are generally appropriate only for the simplest cases, as management can be difficult. Strict uRPF accepts the source address on a datagram if and only if it comes from a direction that would be rational to send a datagram directed to the address, which means that the filter is derived from routing information. These filtering procedures are discussed in more detail in [RFC3704].

In many cases, this router has access to information about what IP prefixes are to be used on a given subnet. This might be because it delegated that prefix through DHCP or monitored such a delegation. It may have advertised that prefix in IPv6 Neighbor Discovery Router Advertisement messages, or monitored such an advertisement. These can be seen as generalizations of the access lists above. When the topology permits, the router can enforce that these prefixes are used by the hosts.

4.1.4. ISP Edge PE Router

An obvious special case of the discussion is with an ISP PE router, where it provides its customer with access. BCP 38 specifically encourages ISPs to use ingress filtering to limit the incidence of spoofed addresses in the network.

The question that the ISP must answer for itself is the degree to which it trusts its downstream network. A contract might be written between an ISP and its customer requiring that the customer apply the procedures of network ingress filtering to the customer’s own network, although there’s no way upstream networks would be able to validate this.

Conversely, if the provider has assigned a single IP address to the customer (for example, with IPv4 NAT in the CPE), PE enforcement of BCP 38 can be on the full address, simplifying many issues.

4.1.5. ISP NNI Router to ISP NNI Router

The considerations explicitly related to customer networks can also be applied to neighboring ISPs. An interconnection agreement might be written between two companies requiring that network ingress filtering policy be implemented on all customer connections. ISPs might, for example, mark datagrams from neighboring ISPs that do not sign such a contract or demonstrably do not behave in accordance with it as ’untrusted’. Alternatively, the ISP might place untrusted prefixes into a separate BGP community [RFC4271] and use that to advertise the level of trust to its BGP peers.

In this case, uRPF is less effective as a validation tool, due to asymmetric routing. However, when it can be shown that spoofed addresses are present, the procedure can be applied.

Part of the complication here is that in the abstract, it is very difficult to know what addresses should appear in packets sent from one ISP to another. Hence, packet-level filtering and enforcement are very difficult at this point in the network. Whether one views this as specific to the NNI, or a general property of the Internet, it is still a major factor that needs to be taken into account.

4.1.6. Cable Modem Subscriber Access

Cable Modem Termination Systems (CMTS) employ Data Over Cable Service Interface Specification (DOCSIS) Media Access Control (MAC) domains. These share some properties with general switched networks, as described above in Section 4.1.1, and some properties with DSL access networks, as described below in Section 4.1.7. They also often have their own provisioning and monitoring tools that may address some of the issues described here.

4.1.7. DSL Subscriber Access

While DSL subscriber access can be bridged or routed, as seen by the service provider’s device, it is generally the case that the protocols carry enough information to validate which subscriber is sending packets. Thus, for ensuring that one DSL subscriber does not spoof another, enforcement can generally be done at the aggregation router. This is true even when there is a bridged infrastructure among the subscribers, as DSL access generally requires all subscriber traffic to go through the access aggregation router.

If it is desirable to provide spoofing protection among the devices within a residence, that would need to be provided by the CPE device, as the ISP's router does not have enough visibility to do that. It is not clear at this time that this problem is seen as a relevant threat.

4.2. Currently Available Tools

There are a number of tools that have been developed, and have seen some deployment, for addressing these attacks.

4.2.1. BCP 38

If BCP 38 [RFC2827] is implemented in LAN segments, it is typically done so on subnetwork boundaries and traditionally relates only to network-layer ingress filtering policies. The result is that hosts within the segment cannot spoof packets from address space outside of the local segment itself; however, they may still spoof packets using sources' addresses that exist within the local network segment.

4.2.2. Unicast RPF

Unicast RPF is a crude mechanism to automate definition of BCP 38 style filters based on routing table information. Its applicability parallels that of BCP 38, although deployment caveats exist, as outlined in [RFC3704].

4.2.3. Port-Based Address Binding

Much of the work of SAVI is initially targeted at minimizing source address spoofing in the LAN. In particular, if mechanisms can be defined to accommodate configuration of port binding information for IP, either to a port, to an unchangeable or authenticated MAC address, or to other credentials in the packet such that an impostor cannot create the needed values, a large portion of the spoofing threat space in the LAN can be marginalized.

However, establishing this binding is not trivial and varies across both topology types and address allocation mechanisms.

4.2.3.1. Manual Binding

Binding of a single link-layer and network-layer address to a port may initially seem trivial. However, two primary areas exist that can complicate such techniques. In particular, these areas involve topologies where more than a single IP-layer address may be associated with a MAC address on a given port, or where multiple hosts are connected via a single physical port. Furthermore, if one or more dynamic address allocation mechanisms such as DHCP are employed, then some mechanism must exist to associate those IP-layer addresses with the appropriate link-layer ports as addresses are allocated or reclaimed.

4.2.3.2. Automated Binding

For IPv4, the primary and very widely used automated address assignment technique is DHCP-based address assignment. This can be coupled with filtering policies that control which hosts can originate DHCP replies. Under such circumstances, SAVI switches can treat DHCP replies as authoritative sources of IP address binding information. By eavesdropping on the DHCP exchanges, the SAVI switch can create the bindings needed for address usage enforcement.

For IPv6, there are two common automated address assignment techniques. While there are many variations and details, for purposes of understanding the threats and basic responses, these are Stateless Address Autoconfiguration (SLAAC) and DHCP-based IPv6 address assignment. For DHCP-based IPv6 address assignment, the techniques above are applicable and suitable.

When SLAAC is used for IPv6 address assignment, the switches can observe the duplicate address detection messages and use those to create the enforcement bindings. This enables the switches to ensure that only properly claimed IP addresses are used for data traffic. It does not enforce that these addresses are assigned to the hosts, since SLAAC does not have a notion of address assignment.

4.2.3.3. IEEE 802.1x

IEEE 802.1x is an authentication protocol that permits a network to determine the identity of a user seeking to join it and apply authorization rules to permit or deny the action. In and of themselves, such tools confirm only that the user is authorized to use the network, but they do not enforce what IP address the user is allowed to use. It is worth noting that elements of 802.1x may well be useful as binding anchors for SAVI solutions.

4.2.4. Cryptographic Techniques

MITM and replay attacks can typically be mitigated with cryptographic techniques. However, many of the applications today either don’t or can’t employ cryptographic authentication and protection mechanisms. ARP for IPv4 does not use such protection. While Secure Neighbor Discovery (SEND) provides such protection for the IPv6 ND protocol, SEND is not widely used to date. Usage of such techniques is outside the scope of this document.

While DNSSEC will significantly help protect DNS from the effects of spoof-based poisoning attacks, such protection does not help protect the rest of the network from spoofed attacks.

4.2.5. Residual Attacks

It should be understood that not all combinations of network, service, and enforcement choices will result in a protectable network. For example, if one uses conventional SLAAC in a switched network, but tries to only provide address enforcement on the routers on the network, then the ability to provide protection is severely limited.

5. Topological Challenges Facing SAVI

As noted previously, topological components and address allocation mechanisms have significant implications on what is feasible with regard to link-layer address and IP address port bindings. The following sections discuss some of the various topologies and address allocation mechanisms that proposed SAVI solutions should attempt to address.

5.1. Address Provisioning Mechanisms

In a strictly static environment, configuration management for access filters that map link-layer and network-layer addresses on a specific switch port might be a viable option. However, most networks, certainly those that accommodate actual human users, are much more dynamic in nature. As such, mechanisms that provide port-MAC-IP bindings need to accommodate dynamic address allocation schemes enabled by protocols such as DHCP, DHCPv6 for address allocation, and IPv6 Stateless Address Autoconfiguration.

5.2. LAN Devices with Multiple Addresses

From the perspective of network topology, consider hosts connected to switch ports that may have one or more IP addresses, and devices that forward packets from other network segments. It is much harder to enforce port-MAC-IP bindings on traffic from such hosts and devices than for traffic from more simply connected devices.

5.2.1. Routers

Routers are the most obvious examples of devices for which it is problematic to implement port-MAC-IP bindings. Routers not only originate packets themselves and often have multiple interfaces, but also forward packets from other network segments. As a result, it’s difficult for port-MAC-IP binding rules to be established a priori, because it’s likely that many addresses and IP subnets should be associated with the port-MAC in question.

5.2.2. NATs

Validating traffic from prefix-based and multi-address NATs is also problematic, for the same reasons as for routers. Because they may forward traffic from an array of addresses, validation requires advance knowledge of the IPs that should be associated with a given port-MAC pair.

5.2.3. Multi-instance Hosts

Another example that introduces complexities is that of multi-instance hosts attached to a switch port. These are single physical devices that internally run multiple physical or logical hosts. When the device is a blade server, e.g., with internal blades each hosting a physical machine, there is essentially a physical switch inside the blade server. While feasible, this creates some complexity for determining where enforcement logic can or should live.

Logically distinct hosts, such as are provided by many varieties of virtualization logic, result in a single physical host and connect to a single port on the Ethernet switch in the topology, actually having multiple internal virtual machines. Each virtual machine may have its own IP and MAC addresses. These are connected by what is essentially (or sometimes literally) an internal LAN switch. While this internal switch may be a SAVI enforcement point to help control threats among the virtual hosts, or between virtual hosts and other parts of the network, such enforcement cannot be counted on in all implementations. If the virtual machines are interconnected by the internal switch, then that logical device is the first switch for the purposes of this analysis.

A further complication with multi-instance hosts is that in many environments, these hosts may move while retaining their IP addresses. This can be an actual relocation of the running software, or a backup instance taking over the functions of the software. In both cases, the IP address will appear at a new topological location. Depending upon the protocols used, it may have the same MAC address or a different one, and the system may or may not issue a gratuitous ARP request after relocation. When such a move is done without changing the MAC address, the SAVI switches will need to update their state. While ARP may be helpful, traffic detection, switch-based neighbor solicitation, interaction with an orchestration system, or other means may be used.

5.2.4. Multi-LAN Hosts

Multi-interface hosts, in particular those that are multihomed and may forward packets from any of a number of source addresses, can be problematic as well. In particular, if a port-MAC-IP binding is made on each of the interfaces, and then either a loopback IP or the address of a third interface is used as the source address of a packet forwarded through an interface for which the port-MAC-IP binding doesn’t map, the traffic may be discarded. Static configuration of port-MAC-IP bindings may accommodate this scenario, although some a priori knowledge of address assignment and topology is required.

While it is rare to use loopback addressing or to send packets out of one interface with the source address of another, these rarities do legitimately occur. Some servers, particularly ones that have underlying virtualization, use loopback techniques for management.

5.2.5. Firewalls

Firewalls that forward packets from other network segments, or serve as a source for locally originated packets, suffer from the same issues as routers.

5.2.6. Mobile IP

Mobile IP hosts in both IPv4 and IPv6 are proper members of the site where they are currently located. Their care-of address is a properly assigned address that is on the link they are using, and their packets are sent and received using that address. Thus, they do not introduce any additional complications. (There was at one time consideration of allowing mobile hosts to use their home address when away from home. This was not done, precisely to ensure that mobile hosts comply with source address validity requirements.) Mobile hosts with multiple physical interfaces fall into the cases above.

Mobile IP Home Agents (HAs) are somewhat more interesting. Although they are (typically) fixed devices, they are required to send and receive packets addressed from or to any currently properly registered mobile node. From an analysis point of view, even though the packets that an HA handles are actually addressed to or from the link the HA is on, it is probably best to think of them as routers, with a virtual interface to the actual hosts they are serving. Thus, if the Mobile IP HA is trusted, it can itself perform IP source address checking on the packets it forwards on behalf of mobile nodes. This would utilize bindings established by the Mobile IP registration mechanisms.

5.2.7. Other Topologies

Any topology that results in the possibility that a device connected to a switch port may forward packets with more than a single source address for a packet that it originated may be problematic. Additionally, address allocation schemas introduce additional considerations when examining a given SAVI solutions space.

5.3. IPv6 Considerations

IPv6 introduces additional capabilities that indirectly complicate the spoofing analysis. IPv6 introduces and recommends the use of SLAAC [RFC4862]. This allows hosts to determine their IP prefix, select an Interface Identifier (IID), and then start communicating. While there are many advantages to this, the absence of control interactions complicates the process of behavioral enforcement.

An additional complication is the very large IID space. Again, this 64-bit IID space provided by IPv6 has many advantages. It provides the opportunity for many useful behaviors. However, it also means that in the absence of controls, hosts can mint anonymous addresses as often as they like, modulo the idiosyncrasies of the duplicate address procedure. Like many behaviors, this is a feature for some purposes and a problem for others. For example, without claiming the entire IID space, an on-link attacker may be able to generate enough IP addresses to fill the Neighbor Discovery table space of the other Layer 3 (L3) devices on the link, including switches that are monitoring L3 behavior. This could seriously interfere with the ability of other devices on the link to function.

6. Analysis of Host Granularity Anti-spoofing

Applying anti-spoofing techniques at the host level enables a site to achieve several valuable objectives. While it is likely the case that for many site topologies and policies full source spoofing protection is not possible, it is also true that for many sites there are steps that can be taken that provide benefit.

One important class of benefit is masquerade prevention. Security threats involving one machine masquerading as another, for example, in order to hijack an apparently secure session, can occur within a site with significant impact. Having mechanisms such that host-facing devices prevent this is a significant intra-site security improvement. Given that security experts report that most security breaches are internal, this can be valuable. One example of this is that such techniques should mitigate internal attacks on the site routing system.

A second class of benefit is related to the traceability described above. When a security incident is detected, either within a site or externally (and traced to the site), it can be critical to determine the actual source of the incident. If address usage can be tied to the kinds of anchors described earlier, this can help in responding to security incidents.

In addition to these local observable benefits, there can be more global benefits. For example, if address usage is tied to anchors, it may be possible to prevent or control the use of large numbers of anonymous IPv6 addresses for attacks, or at least to trace even those attacks back to their source.

As described below in the security considerations, these operational behaviors need to be evaluated in the context of the reduction in user privacy implied if one logs traffic bindings. In particular, in addition to the architectural trade-offs, the network administrator must plan for the proper handling of this relevant privacy information about his users.

7. Security Considerations

This document provides limited discussion of some security threats that source address validation improvements will help to mitigate. It is not meant to be all-inclusive, either from a threat analysis perspective or from the source address validation application side.

It is seductive to think of SAVI solutions as providing the ability to use this technology to trace a datagram to the person, or at least end system, that originated it. For several reasons, the technology can be used to derive circumstantial evidence, but does not actually solve that problem.

In the Internet layer, the source address of a datagram should be the address of the system that originated it and to which any reply is expected to come. But systems fall into several broad categories. Many are single-user systems, such as laptops and PDAs. Multi-user systems are commonly used in industry, and a wide variety of middleware systems and application servers have no users at all, but by design relay messages or perform services on behalf of users of other systems (e.g., SMTP and peer-to-peer file sharing).

Even if every Internet-connected network implements source address validation at the ultimate network ingress, and assurances exist that intermediate devices are to never modify datagram source addresses, source addresses cannot be used as an authentication mechanism. The only techniques for unquestionably validating source addresses of a received datagram are cryptographic authentication mechanisms such as IPsec.

It must be presumed that there will be some failure modes in any SAVI deployment, given the history of technical security mechanisms. A possible attack to be considered by network administrators is an inside attack probing the network for modes of spoofing that can be accomplished. If the probes are conducted at a level below alarm thresholds, this might allow an internal attacker to safely determine what spoof modes he can use. Thus, the use of these techniques must be managed in such a way as to avoid giving a false sense of security to the network administrator.

7.1. Privacy Considerations

It should be understood that enforcing and recording IP address bindings have privacy implications. In some circumstances, this binding data may be considered to be personally identifying information. In general, collecting private information about users brings ethical and legal responsibilities to the network administrator.

For this reason, collection and retention of logged binding information need to be considered carefully. Prevention of spoofing does not in itself require such retention. Analysis of immediate events may rely on having logs of current bindings. Thus, privacy issues can be ameliorated by removing binding logs after the binding lifetimes expire. Logs of apparent spoof attempts are a separate matter and may require longer retention to detect patterns of deliberate or accidental abuse.

With operations of the type described here, the network administrator is collecting information about where on his network the user is active. In addition, the recorded bindings supplement address usage information about users that is available from DHCP logs. For example, if IPv6 SLAAC is being used, and IP to Layer 2 address bindings are being logged, the administrator will have access to information associating users with their IP addresses even if IPv6 privacy addresses are used.

In addition to this, care must be taken in attributing actions to users on the basis of this sort of information. Whatever the theoretical strength of the tools, administrators should always allow for such information being wrong and should be careful about any actions taken on the basis of apparent attribution. These techniques do nothing about address spoofing from other sites, so any evaluation of attribution also needs to allow for such cases.

8. Acknowledgments

A portion of the primer text in this document came directly from [SAVA], authored by Fred Baker and Ralph Droms. Many thanks to Christian Vogt, Suresh Bhogavilli, and Pekka Savola for contributing text and a careful review of this document.

9. References

9.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

9.2. Informative References

[IEEE802.1AX] IEEE, "IEEE Standard for Local and metropolitan area networks - Link Aggregation", IEEE 802.1AX, 2008.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4953] Touch, J., "Defending TCP Against Spoofing Attacks", RFC 4953, July 2007.

[SAVA] Baker, F. and R. Droms, "IPv4/IPv6 Source Address Verification", Work in Progress, June 2007.

[VRSN-REPORT] Silva, K., Scalzo, F., and P. Barber, "Anatomy of Recent DNS Reflector Attacks from the Victim and Reflector Point of View", VeriSign White Paper, April 2006.

Authors’ Addresses

Danny McPherson
VeriSign, Inc.

EMail: dmcpherson@verisign.com

Fred Baker
Cisco Systems

EMail: fred@cisco.com

Joel M. Halpern
Ericsson

EMail: joel.halpern@ericsson.com