Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 29, 2009

M. Bagnulo
UC3M

October 26, 2008

SeND-based Source-Address Validation Implementation
draft-bagnulo-savi-send-00

Status of this Memo

Abstract

This memo describes SeND SAVI, a mechanism to provide source address validation using the SeND protocol. The proposed mechanism is intended to complement ingress filtering techniques to provide a higher granularity on the control of the source addresses used.

Table of Contents

1. Introduction

This memo describes SeND SAVI, a mechanism to provide source address validation for IPv6 networks using the SeND protocol. The proposed mechanism is intended to complement ingress filtering techniques to provide a higher granularity on the control of the source addresses used.

2. Design considerations

2.1. Scope of SeND SAVI

SeND SAVI applicability is limited to IPv6 hosts and IPv6 routers using the SeND protocol [RFC3971].

The application scenario for SeND SAVI is limited to verify the source address of the packets generated by hosts connected to the local link.

In a link there usually are hosts and routers attached. Hosts generate packets with their own address as the source address. This is the so-called local traffic, while routers send packets containing a source address other than their own, since they are forwarding packets generated by other hosts (usually located in a different link). This what the so-called transit traffic.

SeND SAVI allows the validation of the source address of the local-traffic i.e. it allows to verify that the source address of the packets generated by the hosts attached to the local link have not been spoofed. In addition, since SeND does provide the means to verify that a node claiming to act as a router is indeed authorized to act as one, SeND SAVI also provides the means to verify that packets containing off-link prefixes in the source address are generated by authorized routers. However, SeND SAVI does not provide the means to verify if a given (authorized) router is actually

authorized to forward packets containing a specific (off-link) source address Other techniques, like ingress filtering [RFC2827], are recommended to validate transit traffic. In that sense, SeND SAVI complements ingress filtering. Hence, the security level is increased by using these two techniques.

2.2. Constraints for SeND SAVI

SeND SAVI is designed to be susceptible of deployment in existing networks requiring a minimum set of changes. For that reason, SeND SAVI does not require any changes in the hosts which source address is to be verified. Any verification must solely rely in the usage of

already available protocols. This means that SeND SAVI cannot define a new protocol nor to define any new message on existing protocols nor to require that a host uses an existent protocol message in a different way. In other words, the requirement is no host changes. SeND SAVI relies on the usage of the SeND protocol as defined in [RFC3971] and the usage of CGA addresses as defined in [RFC3972]. No changes to SeND or CGAs are required by SeND SAVI

SeND SAVI validation is performed by the SeND SAVI function. Such function can be placed in different type of devices, including a router or a layer-2 bridge. The basic idea is that the SeND SAVI function is located in the points of the topology that can enforce the correct usage of source address by dropping the non-compliant packets.

2.3. Address ownership proof

The main function performed by SeND SAVI is to verify that the source address used in data packets actually belongs to the originator of the packet. Since SeND SAVI scope is limited to the local-link, the originator of the packet is attached to the local-link. In order to to define any source address validation solution, we need to define some address ownership proof concept i.e. what it means to be able to proof that a given host owns a given address in the sense that the host is entitled to send packet with that source address.

Since no hast changes are acceptable, we need to find the means to proof address ownership without requiring a new protocol. In SeND SAVI the address ownership proof is based in the tools used by SeND,

namely CGAs and certificates. CGAs are used to verify that the generator of a packet containing an on-link source address is actually the owner of the address. Certificates are used to verify that a node sending packets with off-link source address is an authorized router. By using these two tools, we can verify the source address used in any packet flowing through the local-link is either generated by the host owner of the on-link source address or is generated by an authorized router.

In both cases, the verification performed applies to the layer-2 address used in the data packets. In the case of the CGA verification, we use CGas and the SeND protocol to verify the Neighbor Advertisement message which contains the binding between the CGA source address and the layer-2 address which will later be used in data packets. By this mean we can verify that is the owner of the CGA source address the one that is claiming to be willing to use the layer-2 address in data packets. We assume that data packets containing this layer-2 information are valid. In the case of the certificate validation, we use the certificate to validate that a

given node is an authorized router. Then we use the CGA of that router to verify the binding between the address of the authorized router and the layer-2 information for that router. After these two checks, we assume that packets containing off-link addresses coming from that layer-2 address are valid, since they come from the layer-2 address of an authorized router.

3. SeND SAVI specification

3.1. SeND SAVI Data structures

SeND SAVI function relies on state information binding the source address used in data packets to the layer-2 information that contained the first packet that used that source IP address. Such information is stored in SeND SAVI Data Base (DB). The SeND SAVI DB will contain a set of entries about the currently used IP source addresses. So each entry will contain the following information:

- IP source address
- Layer-2 address and additional relevant Layer-2 information like the port used in case of switched networks.
- Lifetime

In addition to this, SeND SAVI need to know what are the prefixes that are directly connected, so it maintains a data structure called the SeND SAVI prefix list, which contains:

- Prefix
- Interface where prefix is directly connected
- Lifetime

Finally, SeND SAVI keep a list of the authorized routers that are directly connected. In the SeND SAVI Router List, the following information is stored:

- Router IP address (of the directly connected interface)
- Router Layer-2 address and additional relevant Layer-2 information like the port used in case of switched networks.

3.2. SeND SAVI algorithm

3.2.1. Auhtorized Router Discovery and On-link prefix discovery

In order to be able to determine which devices are entitled to send transit traffic, the SeND SAVI device needs to learn both the set of routers that are connected to the link and the prefixes that are available on-link (in order to be able to differentiate local traffic and transit traffic).

For that the SeND SAVI device MUST listen and process Router

Advertisements (RA) containing the SeND extensions. After the successful validation of the RA message, the advertised prefixes are included in the SeND SAVI prefix list and the router address is included in the SeND SAVI router list, including the associated Layer-2 information.

In addition, the SeND SAVI device MAY send periodic Router Solicitation messages including the SeND extensions to keep the Router list and the prefix list up to date. (Question, should we use the unspecified address for these messages?)

The SeND SAVI function is located in a forwarding device, such as a router or a layer-2 bridge. Upon the reception of a data packet, the packet will be passed to the SeND SAVI function which will perform the processing detailed in this section. The outcome of such

processing can be that the packet is discarded or that is forwarded as usual.

After a data packet is received, the SeND SAVI function checks whether the received data packet is local traffic or transit traffic. It does so by verifying if the source address of the packet belongs to one of the directly connected prefixes available in the receiving interface. It does so by searching the SeND SAVI Prefix List.

- If the IP source address belongs to one of the local prefixes of the receiving interface, the data packet is local traffic and the SeND SAVI algorithm is executed as described next.
- If the IP source address does not belong to one of the local prefixes of the receiving interface, this means that the dat packet is transit traffic. The SeND SAVI verifies if the layer-2 information of the packet corresponds to one of the routers available in the receiving interface, by using the information available in the SeND SAVI router list. If the packet comes from one of the know routers for that interface, then the packet is passed so additional checks such as ingress filtering can be performed. If the packet does not comes from one of the known routers, then the packet SHOULD be discarded.(Note: we could send a RS at this stage to actually verify if the router exists). The SeND SAVI function MAY send an ICMP Destination Unreachable Error with code 5 (Source address failed ingress/egress policy) back to the source address of the data packet.

After checking that the data packet is local traffic, the SeND SAVI function will verify the source address used in the packet. In order to do so, it searches the SeND SAVI DB using the IP source address as a key.

- If no entry is found, the SeND SAVI performs a Neighbor Unreachability Detection procedure as described in [RFC4861] with SeND secured messages as defined in [RFC3971] including the IP

source address and Layer-2 information of the received data packet. If the NUD procedure is successful and also the SeND validation, then a new entry is created, using the information of the data packet, including all the related layer-2 information of where the packet was received from and the lifetime of the entry is set to LIFETIME. The packet is forwarded as usual.

- If an entry is found and the layer-2 information of the received data packet matches to the information contained in the existing

entry, then the lifetime is set to LIFETIME and the packet is forwarded as usual.

- If an entry is found and the layer-2 information of the received data packet does not match the information contained in the existing matching entry, then the SeND SAVI performs a Neighbor Unreachability Detection procedure as described in [RFC4861] with SeND secured messages as defined in [RFC3971] using the IP source address and Layer-2 information available of the received data packet.
  - If the procedure is successful, then the entry information is updated to include also the new information about the data packet received (in particular the new layer-2 information) and lifetime of the entry is updated to LIFETIME. (Note that in this case, the entry may have more than one layer-2 address for the same entry). The packet is forwarded as usual. (Discussion: We could also verify the existing address using NUD for them as well, in order to detect mobility events and discard the ancient location)
  - If the procedure is not successful, then the data packet is discarded. The SeND SAVI function MAY send an ICMP Destination Unreachable Error with code 5 (Source address failed ingress/ egress policy) back to the source address of the data packet.

3.3. SeND SAVI DB maintenance

SeND SAVI SHOULD perform Neighbor Unreachability Detection procedure as defined [RFC4861] in using SeND secured messages periodically for all addresses contained in the SeND SAVI DB. If the NUD procedure is successful, the lifetime value for the entry is updated to LIFETIME. If the procedure is not successful, then the entry is deleted.

4. Handling special cases

SeND SAVI naturally supports the following special cases:

- Mobile nodes are handled naturally, since the node in its new location will pass the NUD procedure and the new location will be included in the SeND SAVI DB. The old entry will be removed by the periodic NUD check. It would be possible to track the location more aggressively by checking the old location when a new

location is verified.

- o Hosts with multiple interfaces connected to the same LAN are compatible with SeND SAVI cause they will be able to pass the NUD procedure, since the host is the owner of the CGA. In this case, the SeND SAVI DB will contain multiple layer-2 addresses for the same IP address.
- o Anycast services can also be supported. In this case, all to nodes should have the CGA keying material, so they all can pass the NUD procedure. As in the previous case, the SeND SAVI DB entry will contain multiple layer-2 addresses for the same IP address.

5. Interaction with FCFS SAVI

TBD

6. Security Considerations

Residual threats.

7. Acknowledgments

Thanks to Ana Kukec for her review and comments on this document.

Marcelo Bagnulo is partly funded by Trilogy, a research project supported by the European Commission under its Seventh Framework Program.

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, May 2000.

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

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

Author's Address

Marcelo Bagnulo
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6248814
Email: marcelo@it.uc3m.es
URI: http://www.it.uc3m.es

Full Copyright Statement

Intellectual Property

ietf-ipr@ietf.org.