Source Address Validation: Use Cases and Gap Analysis

draft-li-sav-gap-analysis-00

Dan Li (Tsinghua)
Jianping Wu (Tsinghua)
Mingqing Huang (Huawei)
Lancheng Qin (Tsinghua)
Nan Geng (Huawei)

Presenter: Lancheng Qin (Tsinghua)
IETF112 - Online
2021.11.09
Background

• The traditional Internet architecture lacks the validation of a packet’s source address
  ✓ Source address spoofing leads to various malicious attacks

• **Source Address Validation (SAV)** is necessary in order to detect and reject spoofed IP packets in the network, and contributes to the security of IP networks (RFC6959)

• Mutually Agreed Norms for Routing Security (**MANRS**) is calling on network operators to implement SAV to prevent source address spoofing

• However, it is difficult to solve the source address spoofing problem at a single "level" or through a single SAV mechanism (RFC5210)
  ✓ It is unrealistic to require a SAV mechanism to be accepted by all network operators
  ✓ The failure of a single SAV mechanism will completely disable SAV
Source address validation architecture (SAVA)

Source Address Validation Architecture (SAVA) [RFC5210] divides SAV into three checking levels and MANRS also follows this architecture:

- **Access network SAV**
  - Source Address Validation Improvement (SAVI) [RFC7039]
    - It is fully effective only when deployed by all access networks
- **Intra-AS SAV**
  - ACL based SAV [RFC2827]
  - Strict uRPF [RFC3704]
- **Inter-AS SAV**
  - EFP-uRPF [RFC8704]
  - Loose uRPF [RFC3704]

It is difficult to require all access networks to deploy SAVI simultaneously, so Intra-AS SAV and Inter-AS SAV are more encouraged by MANRS.
Use cases: Intra-AS and Inter-AS SAV

- **Intra-AS SAV avoids source address spoofing from inner AS**
  - Router1 and Router4 should:
    1. drop the packet with P1' from Router2
    2. accept the packet with P1 from Router3

- **Inter-AS SAV avoids source address spoofing from external ASes**
  - AS1 and AS4 should:
    1. drop the packet with P1'' from AS3
    2. accept the packet with P1 from AS2

*P1 is the source address prefix of Router3*
*P1' is the spoofed P1 by Router2*
*P1'' is the spoofed P1 by routers in AS3*
Existing intra- and inter-AS SAV mechanisms

RFC8704 summarizes the recommendations concerning SAV mechanisms:

• Intra-AS SAV
  ✓ **ACL based SAV** [RFC2827] configures matching rules to specify which source prefixes are acceptable
  ➢ Require manual configuration to update
  ➢ Lacks incentive
  ✓ **Strict uRPF** [RFC3704] takes the source address as a destination address to lookup the FIB and requires the forwarding interface of the FIB matches the incoming interface of the packet

• Inter-AS SAV
  ✓ **EFP-uRPF** [RFC8704] automatically sets a RPF(Reverse Path Filter) list on each **customer interface**
  ✓ **Loose uRPF** [RFC3704] is implemented at **provider and peer interfaces**, which only requires the source address appears in the FIB

However, existing intra- and inter-AS uRPF mechanisms have inherent false positive or false negative problems
Gap analysis: Intra-AS SAV mechanisms

Access network advertises 10.0.0.0/16 to Router 1 while advertises 10.1.0.0/16 to Router 2

Strict uRPF [RFC3704] exhibits false positives in the case of routing asymmetry

When Router3 forwards packets to 10.1.0.0/16
- Forwarding Path: Router3 → Router4 → Router2 → Access network
- Reverse Path: Access network → Router1 → Router3

When Router3 runs strict uRPF, the SAV rule is:
- Packets with source addresses of 10.1.0.0/16 must arrive from Router4
  ✓ The reverse data flow will be dropped

---

Existing intra-AS SAV mechanism has false positive problems
Gap analysis: Inter-AS SAV mechanisms

EFP-uRPF [RFC8704] and loose uRPF [RFC3704] exhibit false negatives when AS4 runs EFP-uRPF at customer interfaces, the SAV rule is:

- Packets with source addresses belonging to AS4’s customer cone can arrive from every customer
  - ✓ ASes in AS4’s customer cone (AS1 and AS2) can forge each other

when AS4 runs loose uRPF at provider and peer interfaces, the SAV rule is:

- Packets with any source addresses existing in FIB can arrive from every provider or peer
  - ✓ ASes outside AS4’s customer cone (AS3 and AS5) can forge any source address in FIB

Existing inter-AS SAV mechanisms have false negative problems
Gap analysis: intra- and inter-AS SAV mechanisms

• An ideal SAV mechanism should guarantee accuracy
  ✓ False positives cause legitimate traffic to be discarded
  ✓ False negatives give attackers the freedom to forge source addresses

• All existing intra- and inter-AS SAV mechanisms cannot guarantee accuracy
  ✓ Intra-AS SAV mechanisms have false positive problems
  ✓ Inter-AS SAV mechanisms have false negative problems

• The root cause of their inaccuracy is that:
  ✓ They all achieve SAV based on local FIB/RIB information which may not match the real data-plane forwarding paths from other sources
Design considerations

• In order to achieve high accuracy ➔ Avoid false positives & Reduce false negatives as much as possible
  ✓ SAV should follow the real data-plane forwarding path

• A path probing method
  ✓ The source router sends probing packets carrying source information. Then each intermediate router can generate SAV rules based on <source information, incoming interface>
  ✓ A combination of allowlist and blocklist can improve the accuracy when forwarding information is incomplete

• Requirements
  ✓ High scalability
    ➢ The design should not induce much overhead (e.g. bandwidth cost of path probing)
  ✓ High deployability
    ➢ The design should generate SAV table automatically and support incremental deployment
  ✓ High security
    ➢ The design should guarantee the integrity of each probing packet (e.g. man in the middle attack)
Next step

• Where to promote this work?
  ✓ Intarea
    ➢ SAVA (source address validation architecture) and SAVI (source address validation improvement) are adopted by intarea
  ✓ RTG
    ➢ Intra-AS SAV and inter-AS SAV are related to routing
  ✓ Opsec
    ➢ EFP-uRPF [RFC8704] is adopted by opsec
  ✓ Others?

• Solicit comments and refine the draft

• Seek collaborators
THANKS!
Questions/Comments?