IETF 122

Source Address Validation Deployment Status

draft-wang-sav-deployment-status-00

Shuai Wang, Dan Li*, Li Chen, Ruifeng Li, Lin He*

Zhongguancun Laboratory and *Tsinghua University

March 20, 2025

https://datatracker.ietf.org/doc/draft-wang-sav-deployment-status/

Previous Presentations

- IETF 118
  - ✓ A Large-scale Measurement of IP Source Spoofing on the Internet
- IETF 119
  - ✓ More Methods to Measure IP Source Outbound Spoofing on the Internet
- IETF 120
  - ✓ Identifying the Presence of Outbound Source Address Validation (OSAV) Remotely
- IETF 121
  - ✓ Remote Measurement of Outbound Source Address Validation Deployment

IETF 122: draft-wang-sav-deployment-status-00

Introduction

- **IP spoofing**, sending packets with source addresses that do not belong to the sending host, **is one of the long-standing security threats in the Internet**
- Source address validation (SAV) is important for protecting networks from IP spoofing attacks
  - Several techniques have been proposed to validate the source address of traffic, e.g., Access Control List (ACL), unicast Reverse Path Forwarding (uRPF), and Virtual routing and forwarding (VRF) table
- outbound SAV (OSAV) and inbound SAV (ISAV)
  - **OSAV:** filtering applied at the network edge to traffic coming from inside the customer network to the outside.
  - **ISAV:** filtering applied at the network edge to traffic coming from the outside to the customer network

Introduction

- The MANRS initiative **considers IP spoofing as one of the most common routing threats**, and defines a recommended action to mitigate spoofing traffic, encouraging network operators to implement SAV for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks.
  - Only 1.6% of routed ASes participate in MANRS, and not all MANRS members follow this action to implement SAV for their networks.
- **There is a lack of comprehensive knowledge regarding the current status of SAV deployment across the Internet community.**
  - **This document aims to provide a comprehensive view about SAV deployment in the Internet**

Measurement methods

ISAV **OSAV**

Deployment status

ISAV **OSAV**

OSAV Measurement Methods

Client-based Method | **Proxy-based Method** | **DNAT-based Method**

- By ***deploying a client on a host*** in the audited network, the client can ***actively generate and send spoofed packets*** to the outside of the audited network
  - **Filtering depth:** A client can incrementally set TTL of spoofed packets, and thus ***its forwarding path can be learned in a way like traceroute***
  - **Filtering granularity:** A client can generate spoofed packets with ***arbitrary IP addresses*** as its source addresses.
  - If a client is installed within a NAT network, spoofed packets may be blocked by the NAT devices
    - Only about half of ASes tested by the CAIDA Spoofer project in 2024 were tested based on public IP addresses.

```
    audited network
+---------------------+                          +--------------------+
|   +-------------+   |          (1)             |   +------------+   |
|   | client IP1  #---|--------------------------|-->#  controlled |   |
|   +-------------+   |   From: forged address   |   | server IP2 |   |
|                     |   To:   IP2              |   +------------+   |
| AS1                 |                          | AS2                |
+---------------------+                          +--------------------+

The client actively sends a set of spoofed packets to the controlled
servers outside of the audited network.
```

Spoofer — Helping to protect your network and the global Internet (BCP 38, caida)

SAV-T Runner

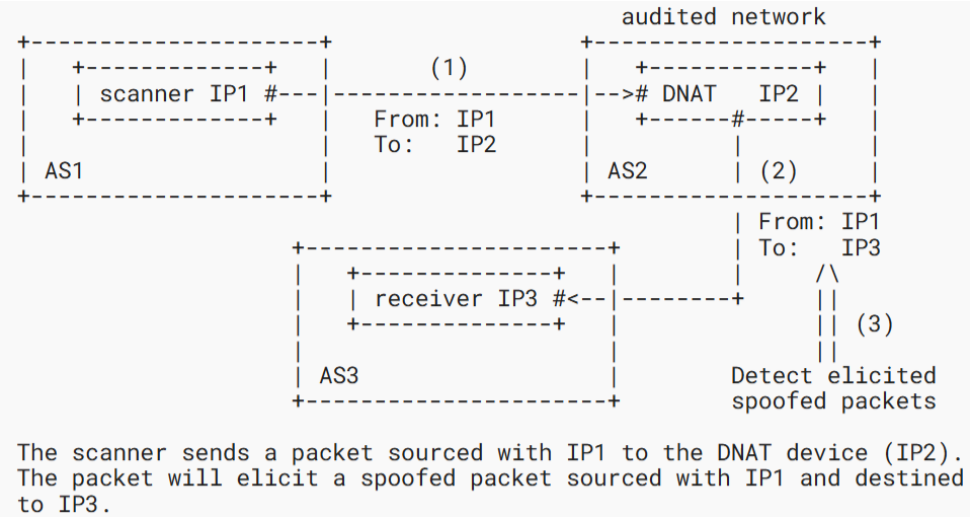
Similarly, by using a controlled server to send spoofed packets to the client, client-based method can measure deployment of **ISAV**.

[1] https://www.caida.org/projects/spoofer/
[2] https://ki3.org.cn/#/sav-t

OSAV Measurement Methods

Client-based Method | **Proxy-based Method** | **DNAT-based Method**

- When matching DNAT rules, the DNAT device changes the packet's destination to a preset address but leaves the source address unchanged ➡ **Spoofed packets**
  - DNAT-based method can utilize various protocols, such as DNS、NTP and TCP, to trigger the audited network into sending spoofed packets.
  - **Filtering depth:** As DNAT devices do not reset the TTL field, the fowarding path taken by spoofed packets can be learned by ***gradually incrementing the initial TTL values*** in original packets
  - **Filtering granularity:** The scanner sends multiple original packets with ***arbitrary source IP addresses***



Similarly, the **proxy-based method** leverages misbehaving DNS proxies, but fails to measure filtering depth and filtering granularity.

[1] Remote Measurement of Outbound Source Address Validation Deployment. draft-wang-savnet-remote-measurement-osav-00

ISAV Measurement Methods

Resolver-based Method | ICMPv6-based Method | IPID-based Method | PMTUD-based Method

- The scanner first sends a DNS query with ***a forged IP address that belongs to the audited network*** (AS2), to a DNS resolver in AS2
  - If the DNS resolver receives the spoofed DNS query, it will send another DNS query to our controlled ADNS

```
                                                audited network
+-----------------+                  +-------------------------+
|  AS1            |                  |  AS2                    |
| +-------------+ |                  |      +-----------+      |
| |   scanner   | |      (1)         |      |  resolver |      |
| |     IP1     #-|----------------->#      IP2     #      |
| +-------------+ |   From:IP3       |      +--+--------+      |
|                 |   To:IP2         |         |               |
+-----------------+                  +------------------------ +
                                                | (2)
                                                V
                                            +----#-----+
                                            |   ADNS   |
                                            +----------+
```

- Then, the scanner send ***a non-spoofed DNS query*** to the same target IP address
  - By ***comparing the results of the spoofed query and the non-spoofed query***, we can infer the deployment of ISAV

```
                                   SPOOFED DNS QUERY

N                                ADNS receives no query    ADNS receives a query
O  D                          +-------------------------------------------------+
N  N   ADNS receives          |                          |                      |
|  S     a query              |        with ISAV         |      without ISAV    |
S                             |                          |                      |
P  Q                          ---------------------------------------------------
O  U   ADNS receives          |                          |                      |
O  E     no query             |         unknown          |      without ISAV    |
F  R                          |                          |                      |
E  Y                          +-------------------------------------------------+
D
```


[1] Nosyk Y, Korczyński M, Lone Q, et al. The closed resolver project: Measuring the deployment of inbound source address validation. IEEE/ACM ToN, 2023

ISAV Measurement Methods

Resolver-based Method | **ICMPv6-based Method** | **IPID-based Method** | **PMTUD-based Method**

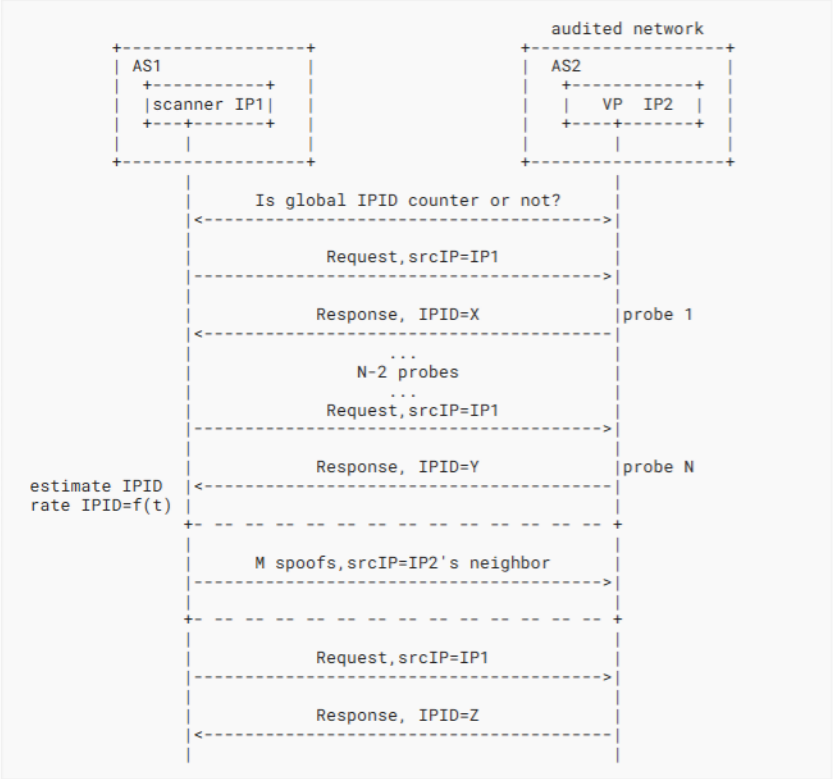
- The scanner sends ICMPv6 packets with forged source address to the target network, and use the ***rate limiting mechanism of ICMPv6*** as an observer to check whether the spoofed packets are received
  - In order to limit the bandwidth and forwarding costs incurred by originating ICMPv6 error messages, an IPv6 node MUST limit the rate of ICMPv6 error messages it originates
  - 3 rounds are conducted, and ***by comparing the number of responses received in different rounds***, we can infer the deployment of ISAV

[1] Long Pan, Jiahai Yang, Lin He, and et. al. Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels. NDSS 2023

ISAV Measurement Methods

Resolver-based Method | **ICMPv6-based Method** | **IPID-based Method** | **PMTUD-based Method**

- The scanner sends packets with forged source address to the target network, and use the ***incremental IPID value*** as an observer to check whether the spoofed packets are received
  - If a server receives a packet, it will increment its global IPID counter by 1, thus leaking information about traffic reaching the server
  - We first estimate the IPID rate of the server, then send *M* spoofed packets to it. **If the spoofed packets reach the server, the IPID will increment by *M***



Similarly, the **PMTUD-based method** send ICMP *Packet Too Big* message with forged source addresses to the server. If the spoofed packets reach the server, the server will reduce the MTU.

[1] Tianxiang Dai, Haya Shulman. Smap: Internet-wide Scanning for Spoofing. ACSAC 2021

Deployment Status - Global Picture

- In February 2025, we used these methods to measure SAV deployment in the Internet
  - ✓ **67.4% of the tested IPv4 and 72.8% of the tested IPv6 ASes lack any ISAV deployment**
  - ✓ **Partial ISAV deployment is observed in 30.2% of IPv4 and 23.1% of IPv6 ASes, suggesting that these ASes deploy ISAV at their access network**
  - ✓ **14.8% of IPv4 ASes and 17.8% of IPv4 /24 prefixes demonstrate complete OSAV deployment**

Category	IPv4 ASes	IPv6 ASes
Deployed	1,157 (2.5%)	372 (4.0%)
Not Deployed	31,817 (67.4%)	6,747 (72.8%)
Partially Deployed	14,235 (30.2%)	2,143 (23.1%)

ISAV deployment status across ASes

Category	IPv4 /24 Prefixes	IPv6 /48 Prefixes
Deployed	222,362 (13.1%)	47,704 (8.1%)
Not Deployed	1,390,206 (82.0%)	404,629 (68.5%)
Partially Deployed	83,460 (4.9%)	138,693 (23.5%)

ISAV deployment status across prefixes

Category	IPv4 ASes	IPv6 ASes
Deployed	409 (14.8%)	318 (71.6%)
Undeployed	2,200 (79.6%)	81 (18.2%)
Partially Deployed	155 (5.6%)	45 (10.1%)

OSAV deployment status across ASes

Category	IPv4 /24 Prefixes	IPv6 /48 Prefixes
Deployed	1,402 (17.8%)	679 (80.9%)
Undeployed	6,335 (80.4%)	130 (15.5%)
Partially Deployed	140 (1.8%)	30 (3.6%)

OSAV deployment status across prefixes

Deployment Status - Global Picture

- 91.52% of the tested IP addresses deploy OSAV within 2 hops from the endpoints
- The prefix length of /20-/24 dominates OSAV deployment (55%)
  - ✓ These prefix lengths correspond to standard IPv4 allocation units for ASes. Hence, this suggests OSAV is predominantly deployed at **AS border interfaces**
- 41.66% of networks filter inbound spoofing packets at /29-/30 granularity
  - ✓ This suggests ISAV is predominantly deployed in **access networks**

Hop	Percentage
1	66.01 %
2	25.51 %
3	4.58 %
4	2.46 %
5	1.03 %
6	0.14 %
7	0.00 %
8	0.21 %
9	0.07 %
10	0.00 %

OSAV filtering depth (IPv4)

Range	Percentage
/ 8	0.13 %
/ 9	0.26 %
/10	0.53 %
/11	0.13 %
/12	0.26 %
/13	0.66 %
/14	0.79 %
/15	0.53 %
/16	3.95 %
/17	4.74 %
/18	3.29 %
/19	5.53 %
/20	6.97 %
/21	8.55 %
/22	23.95 %
/23	7.76 %
/24	8.29 %
/25	2.24 %
/26	2.63 %
/27	3.95 %
/28	3.29 %
/29	5.79 %
/30	3.42 %
/31	2.37 %

OSAV filtering granularity (IPv4)

Range	Percentage
/ 8	0.17 %
/ 9	1.99 %
/10	6.07 %
/11	4.48 %
/12	4.94 %
/13	3.50 %
/14	3.99 %
/15	5.78 %
/16	2.17 %
/17	3.27 %
/18	2.76 %
/19	2.43 %
/20	1.84 %
/21	3.25 %
/22	1.73 %
/23	3.24 %
/24	1.55 %
/25	0.97 %
/26	1.02 %
/27	1.35 %
/28	1.85 %
/29	22.94 %
/30	18.72 %

ISAV filtering granularity (IPv4)

Deployment Status - Deployment in Countries/Regions

- China, South Korea, and France demonstrate higher OSAV deployment ratios, while Russia, Brazil, and India show lower OSAV deployment ratios
- ISAV deployment remains limited in most regions, with South Korea, Chinese Taiwan and Poland exhibiting more advanced ISAV deployment

country/region	OSAV Tested Prefixes	OSAV Deployment Ratio
CN	376	76.3%
KR	58	75.9%
FR	12	75.0%
DE	16	68.8%
US	300	42.7%
NL	18	33.3%
PL	70	32.9%
CA	117	32.5%
GB	28	32.1%
AU	11	27.3%
IT	116	23.3%
TW	19	21.1%
EG	56	19.6%
ID	490	17.8%
JP	17	17.6%
MX	36	13.9%
ES	38	10.5%
RU	75	9.3%
BR	2,575	7.3%
IN	1,430	5.5%

OSAV deployment

country/region	ISAV Tested Prefixes	ISAV Deployment Ratio
KR	71,934	44.8%
TW	22,523	42.0%
PL	17,880	40.5%
EG	16,806	37.3%
FR	35,220	19.4%
DE	49,956	14.4%
ES	15,018	16.2%
BR	47,874	11.8%
US	562,655	10.2%
RU	56,084	10.2%
AU	21,023	8.3%
NL	19,803	8.3%
CA	23,801	7.2%
GB	31,271	6.9%
JP	67,173	6.2%
IT	30,357	5.7%
CN	211,539	4.8%
ID	18,845	4.6%
IN	30,569	4.1%
MX	17,665	3.4%

ISAV deployment

Deployment Status - Comparison between ISAV and OSAV

- G-Network (AS272122), DigitalOcean (AS14061), Korea Telecom (AS4766) and China Telecom (AS4134) achieve over 90% OSAV deployment
- Chungwa Telecom (AS3462), Korea Telecom (AS4766), Charter (AS20115), and Comcast (AS7922) demonstrate significantly higher ISAV deployment

ASN	OSAV Tested Prefixes	OSAV Deployment Ratio
272122	160	100.0%
14061	37	100.0%
4766	36	97.2%
4134	232	92.7%
4837	48	81.2%
17995	71	74.6%
15924	56	26.8%
8452	49	12.2%
38758	47	4.3%
150008	102	0.0%
34984	78	0.0%
52468	66	0.0%
395582	64	0.0%
58659	55	0.0%
23688	43	0.0%
18229	40	0.0%
52444	36	0.0%
133676	34	0.0%
23923	33	0.0%
18002	33	0.0%

OSAV deployment

ASN	ISAV Tested Prefixes	ISAV Deployment Ratio
3462	12,752	70.1%
4766	37,667	60.8%
20115	13,505	40.1%
7922	29,403	22.9%
8075	22,415	10.0%
209	11,435	7.9%
12389	12,288	5.0%
3320	14,684	4.7%
4134	69,625	4.4%
4837	48,749	4.0%
7018	31,888	3.3%
4713	14,727	3.2%
16509	48,563	3.2%
45090	11,168	3.0%
3269	14,181	3.1%
701	15,694	2.2%
17676	11,702	1.8%
8151	11,996	1.6%
749	70,399	1.2%
36947	11,339	0.4%

ISAV deployment

Deployment Status - Comparison between ISAV and OSAV

- We find a positive correlation between the deployment of OSAV and ISAV
  - **10.9%** of ASes that deploy ISAV also deploy OSAV, while only **5.9%** of ASes without ISAV deploy OSAV
  - **36.0%** of ASes that deploy OSAV also deploy ISAV, while only **22.6%** of ASes without OSAV deploy ISAV

Deployment Status - Impact of MANRS

- To understand the impact of MANRS on SAV deployment, we compare SAV deployment ratios between MANRS and non-MANRS networks, including both full and partial deployments
- MANRS networks demonstrate superior SAV deployment
  - For OSAV, **29.1%** in MANRS networks versus **19.6%** in non-MANRS networks
  - For ISAV, **73.3%** in MANRS networks versus **56.7%** in non-MANRS networks
- These results indicate that ***although anti-spoofing is a recommended action, MANRS participation improves SAV deployment across network configurations***.

	OSAV Deployment Ratio	ISAV Deployment Ratio
MANRS	29.1%	73.3%
Non-MANRS	19.6%	56.7%

If you are interested in collaborating or have suggestions on how we can enhance our measurement framework, please reach out to us!

Thanks!

wangshuai@zgclab.edu.cn