IETF 121

Remote Measurement of Outbound Source Address Validation Deployment

draft-wang-savnet-remote-measurement-osav-00

Shuai Wang, Dan Li*, Li Chen, Ruifeng Li, Qian Cao

Zhongguancun Laboratory and *Tsinghua University

November 4, 2024

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

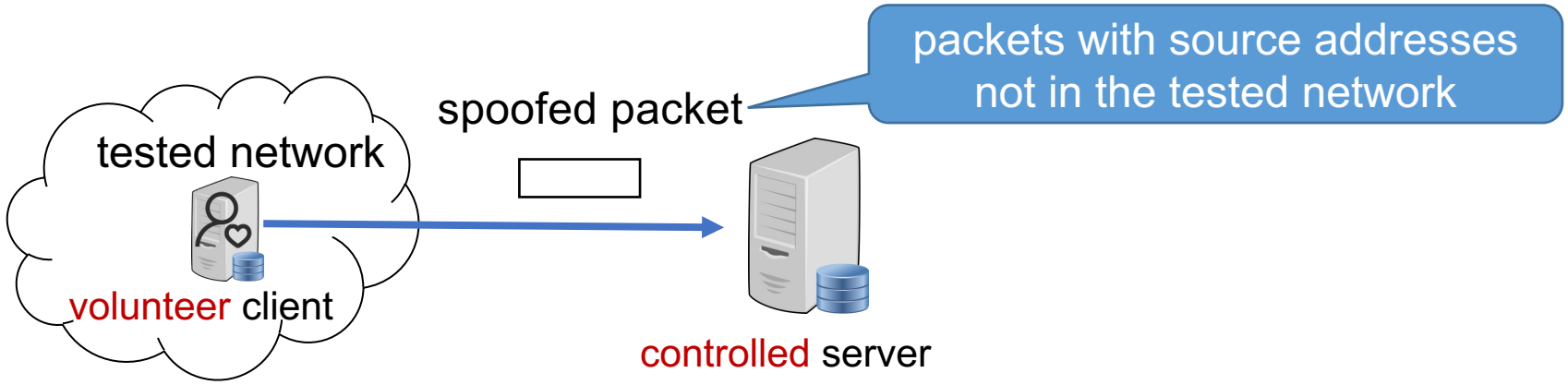
IETF 121: draft-wang-savnet-remote-measurement-osav-00

Motivation

- Outbound IP spoofing, where attackers send packets with forged source IP addresses, poses a significant threat to Internet security.
  - ✓ Malicious users often use IP spoofing to carry out attacks like reflective DDoS or DNS cache poisoning.
- Measuring the deployment of outbound source address validation (OSAV) is critical for characterizing the vulnerability to outbound IP spoofing across the global Internet.
  - ✓ Network operators are often reluctant to implement it due to concerns about validation accuracy, operational overhead, and the risk of accidentally dropping legitimate traffic.
- Remote measurement of OSAV deployment offers a practical method for measuring numerous ASes efficiently.

Why is Local Measurement Not Enough?

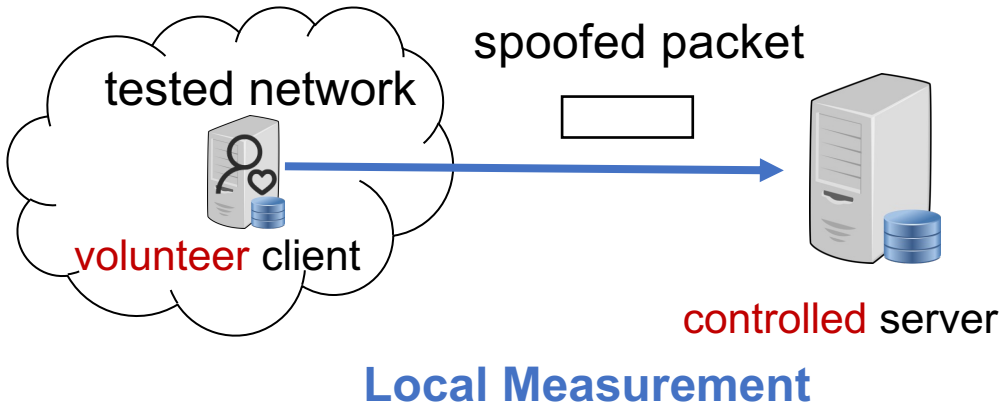
- To measure if a network can send spoofed packets, one can try to send spoofed packets to controlled servers and observe whether they are received.
  - ✓ **Local measurement:** If a volunteer in a network can deploy software that actively sends spoofed packets to a controlled server, the network's outbound IP spoofing capability can be easily measured, which is how CAIDA's Spoofer tool operates.
  - ✓ **Poor scalability:** This volunteer-based approach does not scale well because it is difficult to obtain cooperation from a large number of networks.

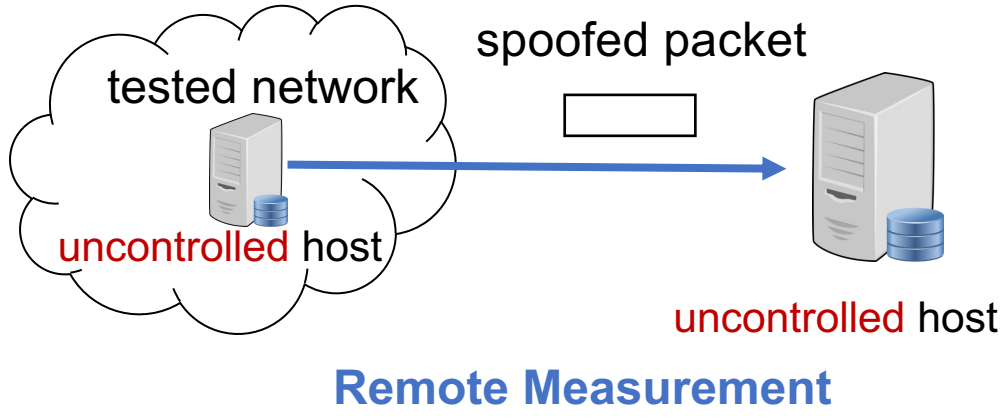


Local Measurement

Remote Measurement Needs No Cooperation

- It is essential to develop methods for remotely measuring outbound IP spoofing without relying on active participation from volunteers in the tested networks.
  - ✓ **Remote measurement:** If uncontrolled hosts in the tested network can be elicited to send spoofed packets to hosts outside the tested network, it will be possible to measure the deployment of OSAV without cooperation with the tested network.

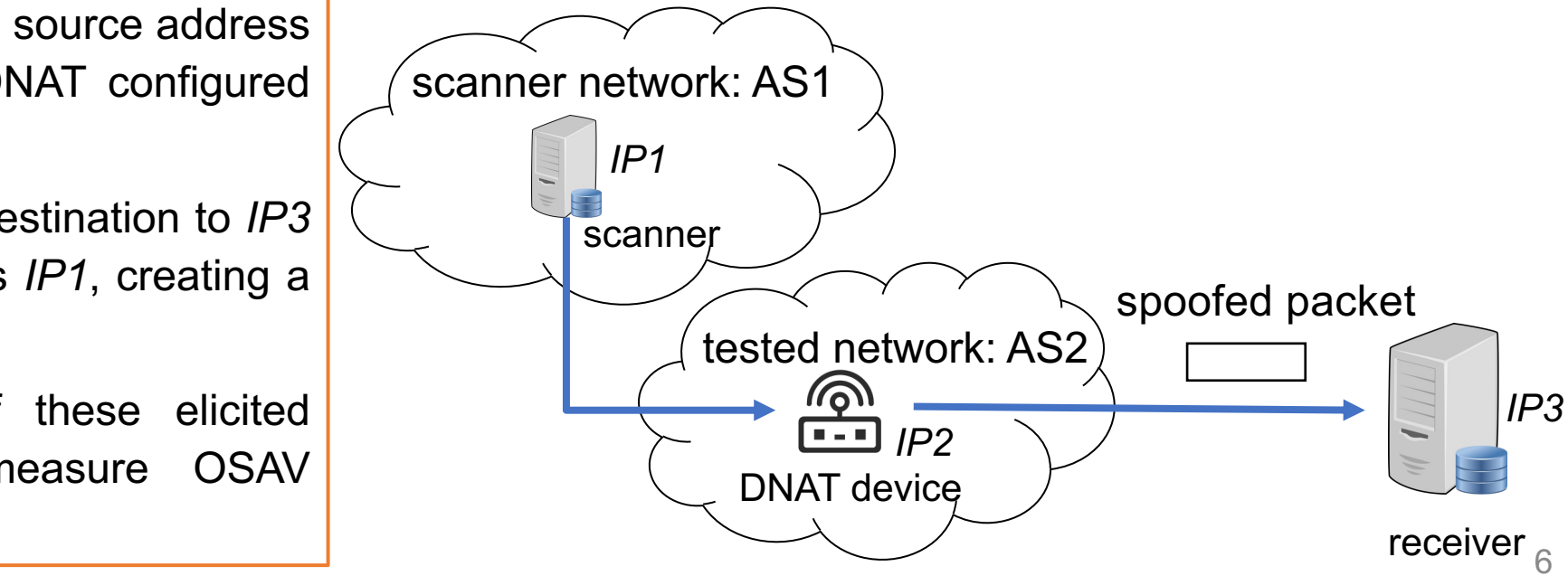




Basic Setup

- To remotely measure OSAV deployment, we use **destination network address translation (DNAT)** to elicit remote hosts to sending spoofed packets.
  - ✓ When a packet matches DNAT rules, the DNAT device changes the packet's destination to a preset address, while leaving the source address unchanged.
  - ✓ This results in a spoofed packet because the source address does not belong to the network.

- The scanner sends a packet with source address *IP1* to a network device with DNAT configured (*IP2*).
- The DNAT device modifies the destination to *IP3* but keeps the source address as *IP1*, creating a spoofed packet.
- By observing the behavior of these elicited spoofed packets, we can measure OSAV deployment in AS2.

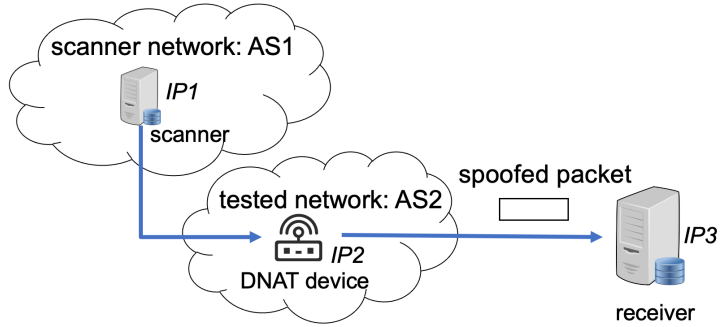


How to Characterize Deployment Status

- Presence/Absence of OSAV
  - ✓ **Presence of OSAV:** A SAV mechanism is deployed in the network.
  - ✓ **Absence of OSAV:** No SAV mechanism is deployed in the network.
- Filtering depth
  - ✓ The position where a spoofed packet is discarded when going out of the network.
- Filtering granularity
  - ✓ The range of IP addresses that can be spoofed as. For example, if the filtering granularity is /8, addresses within the same /8 prefix as the original IP address will not be discarded.

Presence/Absence of OSAV

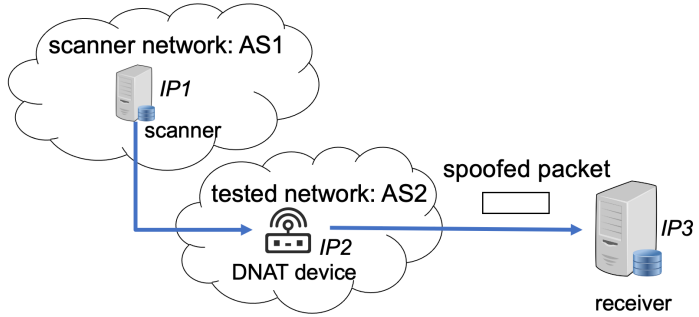
- If the elicited spoofed packets reach the receiver IP3
  - ✓ OSAV is not deployed in AS2, i.e., absence of OSAV.
- If the elicited spoofed packets do not reach the receiver IP3
  - ✓ OSAV is deployed in AS2, i.e., presence of OSAV, so that the spoofed packets are discarded.
  - ✓ or, no spoofed packet is generated.



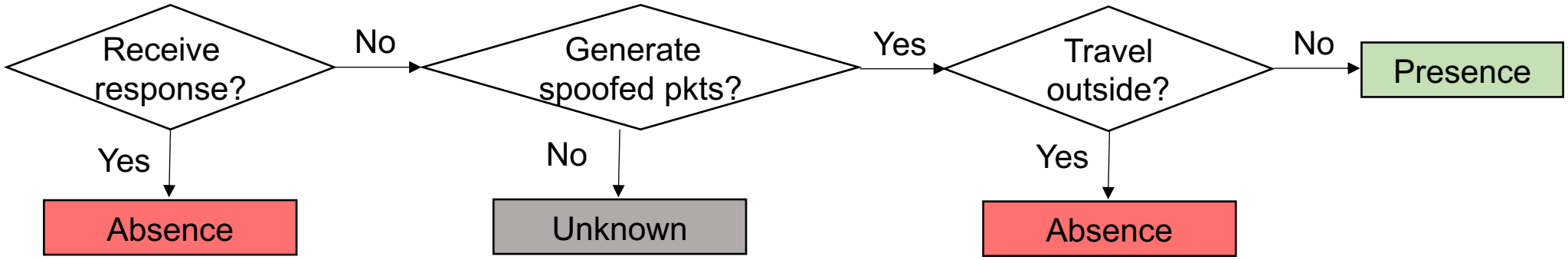
- To confirm the generation of a spoofed packet, we leverage the ICMP time exceeded message, which quotes the first 28 bytes of the original packet that triggers time exceeded message.
  - ✓ We can learn the source IP address and destination IP address of the original packet from the quotation.
  - ✓ If the destination IP address has been changed while the source IP address remains IP1, we can confirm that a spoofed packet was generated.

Presence/Absence of OSAV

- If the receiver does not give a response when the spoofed packet reaches it, we can still infer the deployment of OSAV by analyzing the path of the spoofed packet.
  - ✓ If OSAV is absent, the spoofed packet will travel beyond AS2.
  - ✓ Otherwise, it will be blocked and never leave AS2.



Workflow Overview

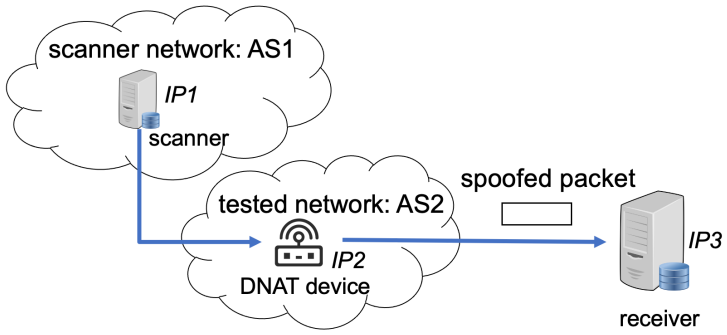


Filtering Depth

- To measure filtering depth, we first obtain the path of the spoofed packet, and then take the last responsive hop as the position where filtering happens.
  - ✓ Since DNAT devices do not reset the TTL field in packets they receive, we increment the initial TTL value in original packets, similar to how traceroute works.
  - ✓ By collecting the source IP addresses from the ICMP time exceeded messages, we can trace the path of the spoofed packet.
  - ✓ Note that some hops may not respond when TTL expires, leading to a conservative estimate of the filtering depth. In such cases, the actual distance the spoofed packet travels could be farther than the inferred distance.

Filtering Granularity

- To measure filtering granularity, spoofed packets with various source IP addresses need to be sent. To this end, the scanner needs to send multiple original packets, using not only IP1 (scanner's IP) but also other addresses adjacent to IP2 (DNAT device's IP) as the source addresses.
  - ✓ When other adjacent addresses are used, the scanner will not receive a response, as the source IP seen by the receiver is not IP1.
  - ✓ To detect whether these spoofed packets reach the receiver, we use specific protocols.
    - ➢ For example, if the receiver is a DNS resolver, and the spoofed packet is a DNS query, the resolver will forward the query to the authoritative DNS server. By querying a domain under our control, we can determine if the spoofed packet reached the receiver.
    - ➢ Additionally, methods used for inbound SAV measurement, such as increases in IP-ID, ICMP fragmentation, or ICMP rate limiting, can help confirm whether the spoofed packets arrived.



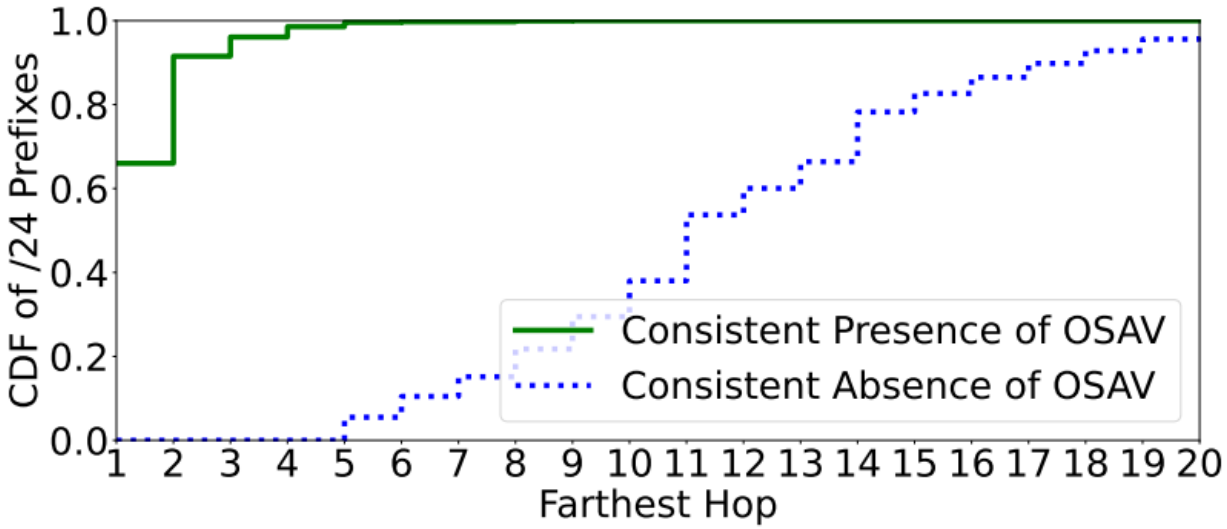
Measurement Result

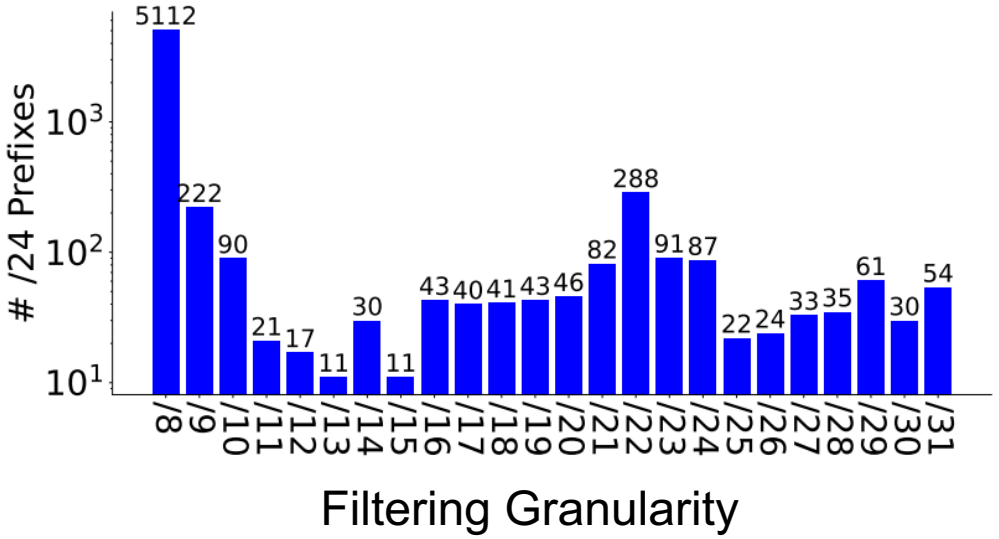
- **Consistent presence of OSAV:** all DNAT devices within the prefix/AS cannot send spoofed packets outside the AS.
- **Consistent absence of OSAV:** all DNAT devices within the prefix/AS can send spoofed packets outside the AS
- **Partial absence of OSAV:** some DNAT devices within the prefix/AS can send spoofed packets outside the AS, while others cannot.

Consistent presence		Partial absence		Consistent absence		Total	
Prefixes	ASes	Prefixes	ASes	Prefixes	ASes	Prefixes	ASes
1,617 (17%)	404 (12%)	313 (3%)	274 (8%)	7,678 (80%)	2,620 (80%)	9,608	3,298

- 86% of ASes tested by us were not covered by CAIDA Spoofer in the last year.
- 80% of tested ASes show the consistent absence of OSAV, indicating a still severe OSAV deployment situation

Measurement Result





- 66% of OSAV deploys at the first hop, and only 3.9% of OSAV is deployed beyond three hops from the DNAT devices.
- Most DNAT devices can spoof with addresses in small lengths of prefixes, e.g., /8 and /9, indicating that their networks allow a large range of spoofed addresses.

Next Step

☐Seek feedback and comments

- ✓ The measurement results are published at https://ki3.org.cn/#/sav and updated monthly.
- ✓ We seek feedback and comments about not only our solutions but also our measurement results.

☐Collaborations are welcome

- ✓ We invite the community to participate in remote measurement of OSAV deployment.

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