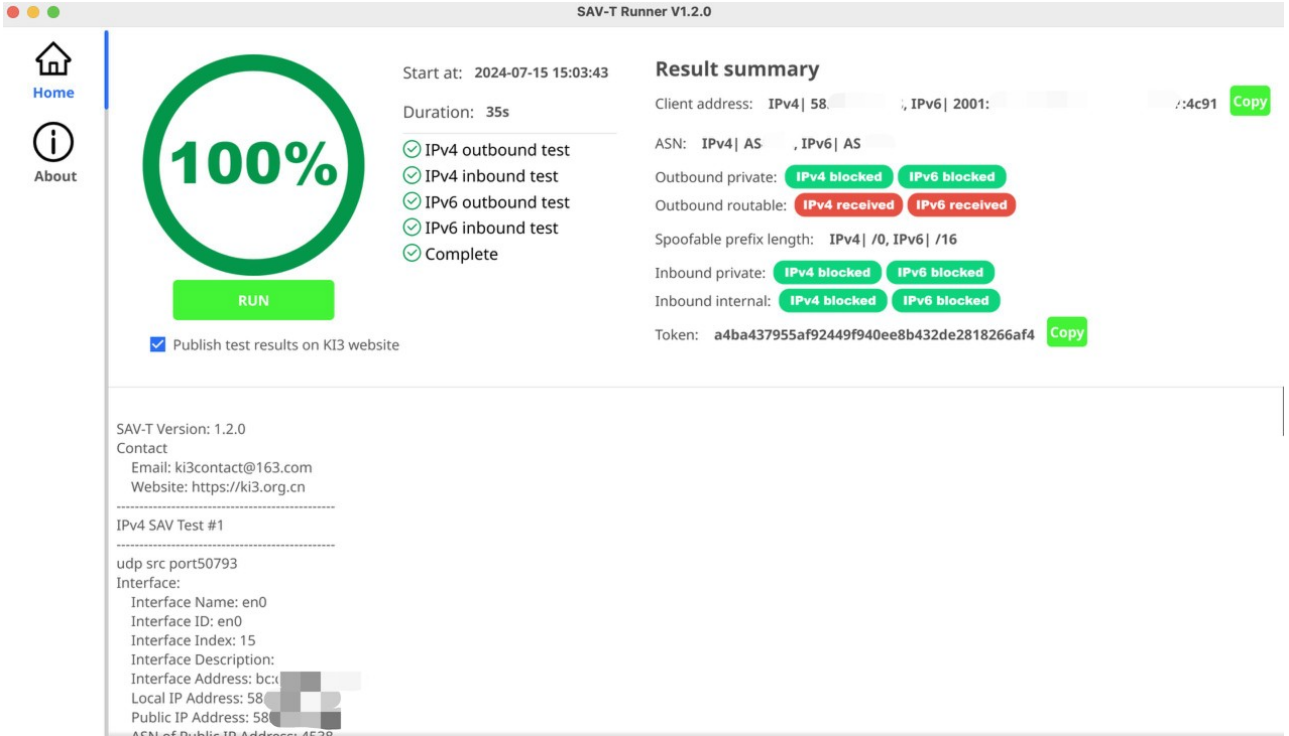
# Measuring SAV deployment with SAV-T

Ruifeng Li
Zhongguancun Laboratory

July 23, 2024

# What is SAV-T

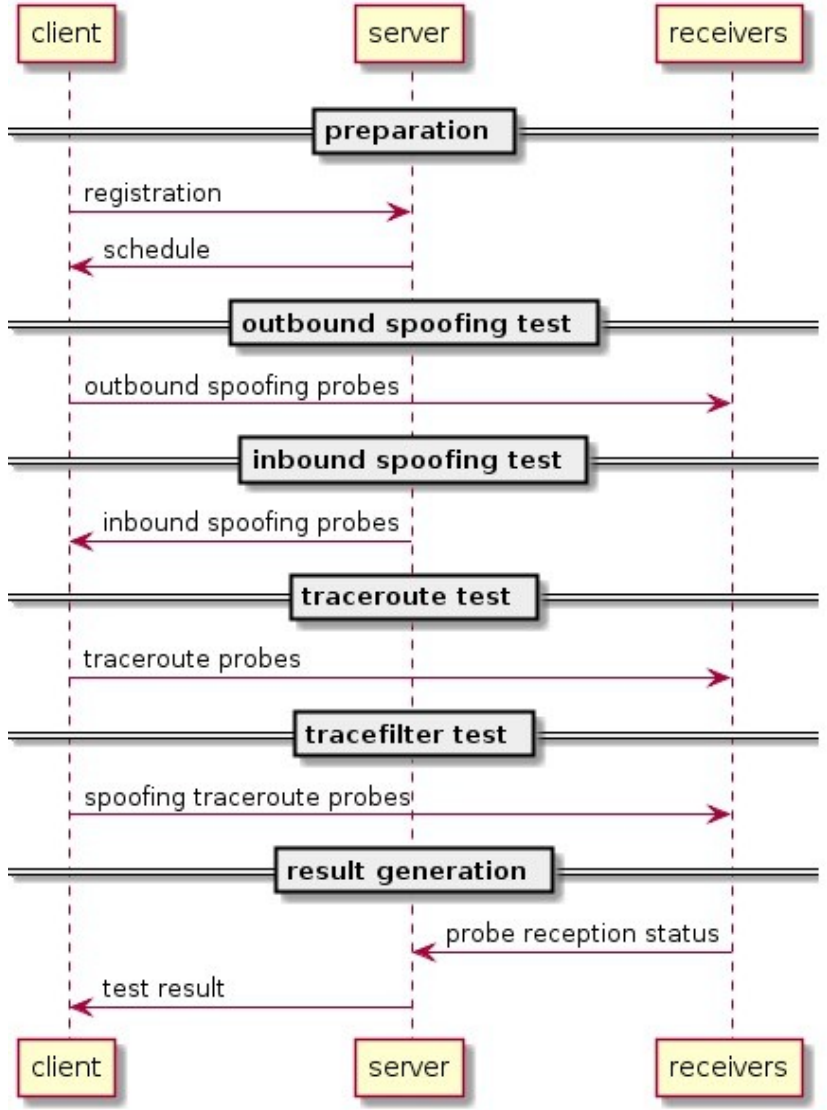
- SAV-T is a platform for testing and disclosing deployment data of source address validation
  - ✓For testing, SAV-T client is easy to install and runs on one click.
  - ✓For disclosing, SAV-T collects users' testing data for research use only and discloses data with users' permission.
- SAV-T can test
  - ✓private & routable
  - ✓inbound & outbound
  - ✓IPv4 & IPv6
  - ✓spoofable prefix length



# How does SAV-T work

- SAV-T controls three characters: **client**, **server** and **receivers**.

1. **Client** registers a new measurement routine in **server**.
2. **Server** sends the schedule (which addresses to spoof) to **client**.
3. **Client** sends packets sourced with scheduled addresses to **receivers**. (**outbound spoofing test**)
4. **Server** sends spoofed packets sourced with address that is in the same network with **client**. (**inbound spoofing test**)
5. **Client** sends traceroute probes to **receivers**. (**traceroute test**)
6. **Client** sends tracefilter probes to **receivers**. (**tracefilter test**)
7. **Receivers** return the probe reception status to **server**.
8. **Server** returns test result to **client**.

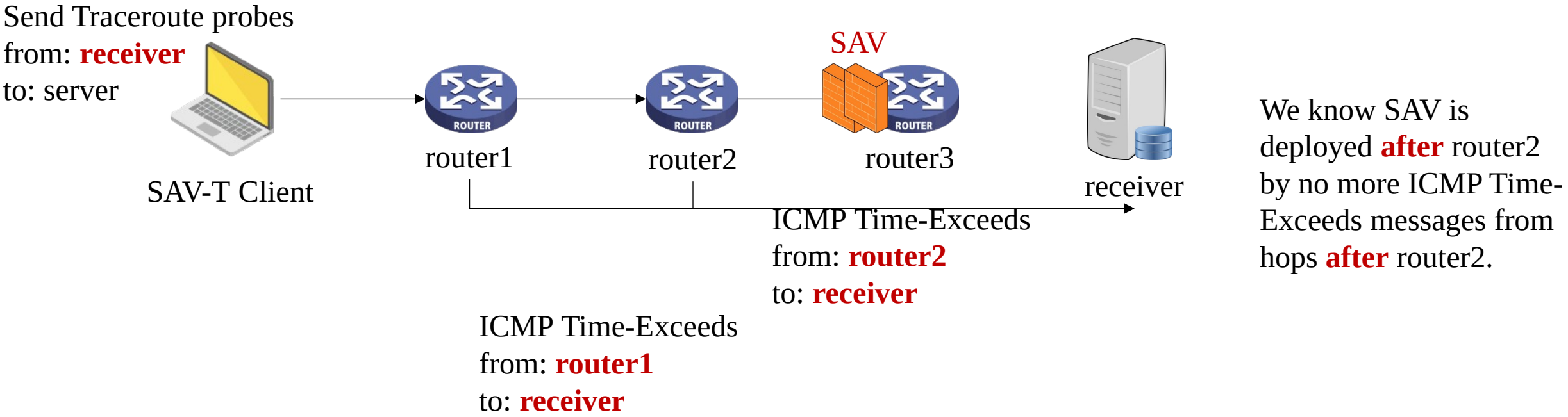


# How does SAV-T work

- To identify the spoofable prefix length which is the length of the largest prefix that the client can spoof, SAV-T client
  - ✓ sends packets sourced with a series of addresses which are only **one-bit different** from the client's address.
- SAV-T identifies a network does not deploy outbound SAV if
  - ✓ the client can spoof a **routable** address which does not belong to the client's AS.
- SAV-T identifies a network does not deploy inbound SAV if
  - ✓ the client can receive the spoofed packets sourced with the address in the same network from our receivers.

# How does SAV-T work

- To perform traceroute, SAV-T
  - ✓uses **Dublin Traceroute** to traceroute with the ability to detect Network Address Translation (NAT)
- To perform tracefilter which can infer the position of SAV, SAV-T
  - ✓sends traceroute probes **sourced with our receivers**.




We know SAV is deployed **after** router2 by no more ICMP Time-Exceeds messages from hops **after** router2.

# How does SAV-T disclose measurement results

- SAV-T will only disclose outbound SAV data on users' permission

**SAV-T Testing Report**

**Summary**

- Session information
  - Test run time: **2024-07-12 18:38:13**
  - Client prefix (IPv4): **223.72.89.x/24**
  - Client AS (IPv4): AS56048 **(CMNET-BEIJING-AP)**
  - IPv4 probes: **35**
  - Client prefix (IPv6): **2409:8a00:18xx::/40**
  - Client AS (IPv6): AS56048 **(CMNET-BEIJING-AP)**
  - IPv6 probes: **19**

Packets with spoofed private IPv6 address will be blocked

- Outbound spoofing summary
  - Private - RFC1918: IPv4 rewritten | IPv6 blocked
  - Routable: IPv4 rewritten | IPv6 received
  - Larg… spoofable neighbor prefix leng… IPv4 None | IPv6 /8

The client can spoof addresses in the same /8 prefix.

NAT rewrites every packets' src and we cannot know the situation of SAV deployment

Packets with spoofed routable IPv6 address will not be blocked

- IPv6 probe testing

| Spoofed source address | Destination | Received |
|---|---|---|
| fdc1:d53a:9019:0:f6ec:6b3b:df01:1ae4 | 240b:4001:21b:1501:5b7a:abd3:5e30:395b | No |
| 2408:4006:1210:7c00:4632:d4b7:9509:d068 | 240b:4001:21b:1501:5b7a:abd3:5e30:395b | Yes |
| 2605:6400:20:9d:2d8c:6f33:f4db:ab02 | 240b:4001:21b:1501:5b7a:abd3:5e30:395b | Yes |

One private address to spoof with

Two routable addresses to spoof with

Not Received

Received

# How does SAV-T disclose measurement results

We hide the low 88 bits to protect users' privacy.

- IPv6 adjacent prefix testing

| Spoofed source address | Destination | Prefix length | ASN of spoofed source address | Received |
|---|---|---|---|---|
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 120 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 112 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 104 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 96 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 88 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 80 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 72 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 64 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 56 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 48 | AS56048 | Yes |
| 2409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 40 | AS56048 | Yes |
| 2409:8a00:98xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 32 | AS56048 | Yes |
| 2409:8a80:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 24 | AS9808 | Yes |
| 2409:a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 16 | AS13030 | Yes |
| 2489:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 8 | AS9498 | Yes |
| a409:8a00:18xx::/40 | 240b:4001:21b:1501:5b7a:abd3:5… | 0 | AS4466 | No |

Orange Yes means the spoofed packet is received but the source address is in the same AS with the client.

A Red Yes means the spoofed packet is received and the source address is in the different AS from the client.

# What's next for

?

- We are still working on tracefilter.
- How to promote SAV-T
  - ✓We are seeking cooperations with universities.
  - ✓We are working on distributing the measurement tasks on crowdsourcing platforms like MTurk.
  - ✓We are trying to contact network operators via emails.

- Thanks for your listening!
- You can download SAV-T on our website:

  https://ki3.org.cn/#/ipSourceVerification?sub=savTest&children=clientDownload
- Email: lirf@mail.zgclab.edu.cn