SPOOFER Protect your network and the global Internet

An independent source of data on IP source address validation

https://spoofer.caida.org

PROTECT YOUR NETWORK

Prevent attackers from weaponizing your network resources against you, by ensuring your network performs source address validation (SAV) on **inbound** packets

PROTECT THE INTERNET

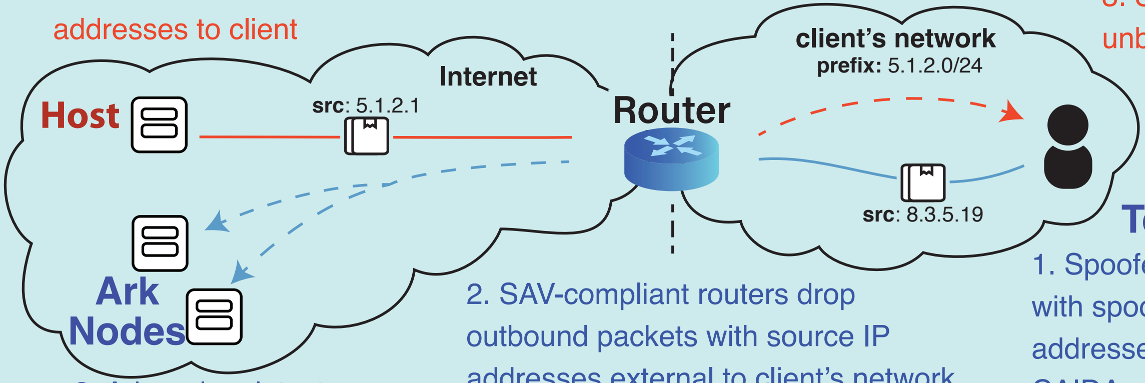
Mitigate global security threats caused by IP spoofing, by ensuring your network performs source address validation on **outbound** packets

Testing inbound SAV

1. CAIDA host attempts to send packets with spoofed client's network source IP addresses to client

2. SAV-compliant routers drop inbound packets with source IP addresses internal to client's network.

3. Spoofer client detects unblocked spoofed packets.

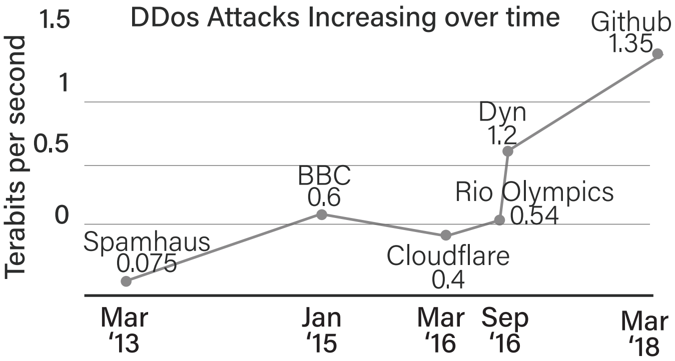


Testing outbound SAV

1. Spoofer client sends packets with spoofed external source IP addresses outbound to CAIDA-controlled nodes.

2. SAV-compliant routers drop outbound packets with source IP addresses external to client's network.

3. Ark nodes detect unblocked spoofed packets.



Ensure that your network does not contribute to launching the next Distributed Denial of Service (DDoS) attack by adding the free, open-source measurement tool, Spoofer, to your security tool chest! **SAV deployment protects your customers** who might otherwise be complicit in launching spoofed DDoS attacks!

UC San Diego SDSC SAN DIEGO SUPERCOMPUTER CENTER caida

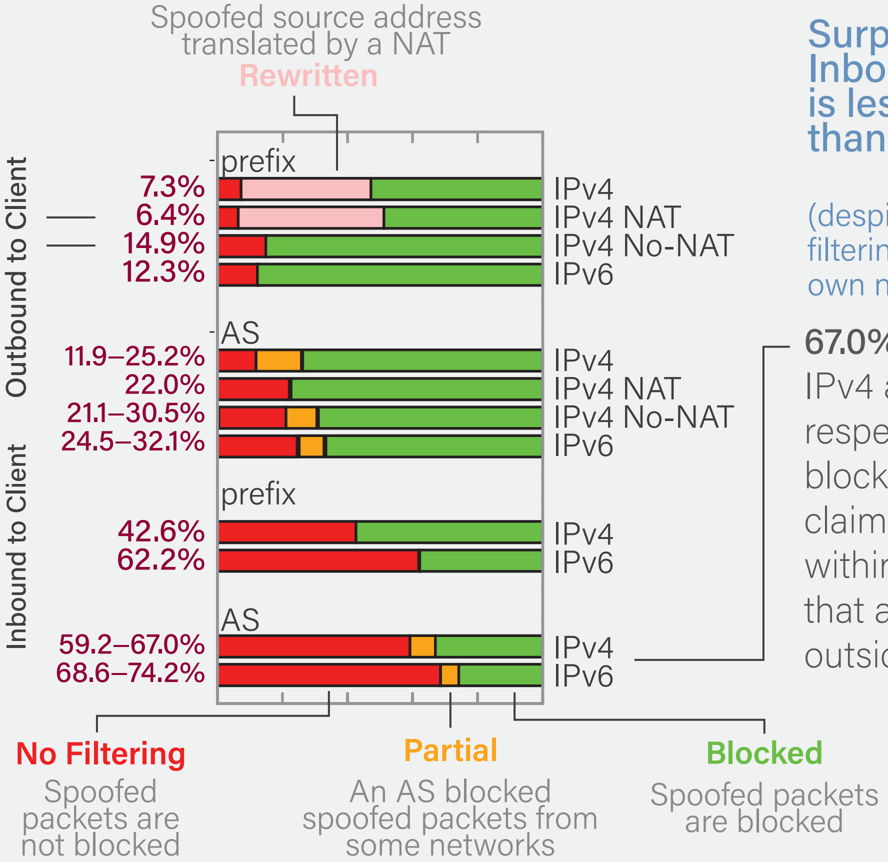
The Center for Applied Internet Data Analysis (CAIDA) conducts network research and builds research infrastructure to support large-scale data collection, curation, distribution and scientific analysis. Located at the San Diego Supercomputer Center at UC San Diego, CAIDA designs, deploys and maintains computational, data analysis and visualization services that illuminate the most pressing problems of today's Internet infrastructure.

What we have inferred from our measurements

NAT does not block ability to spoof in IPv4

Could spoof from **6.4%** of observed IPv4/24 prefixes where NAT was present

Could spoof from **14.9%** of observed IPv4/24 prefixes where NAT was not present



Surprisingly, Inbound filtering is less deployed than outbound!

(despite that inbound filtering protects one's own network!)

67.0% and **74.2%** of IPv4 and IPv6 ASes, respectively, do not block packets that claims to be from within their network that arrive from outside their network

What regulators, policy makers, public interest, and insurance industry need to know

Market forces alone will not remedy the harm that networks without SAV pose to the Internet, and to commerce that relies on it.

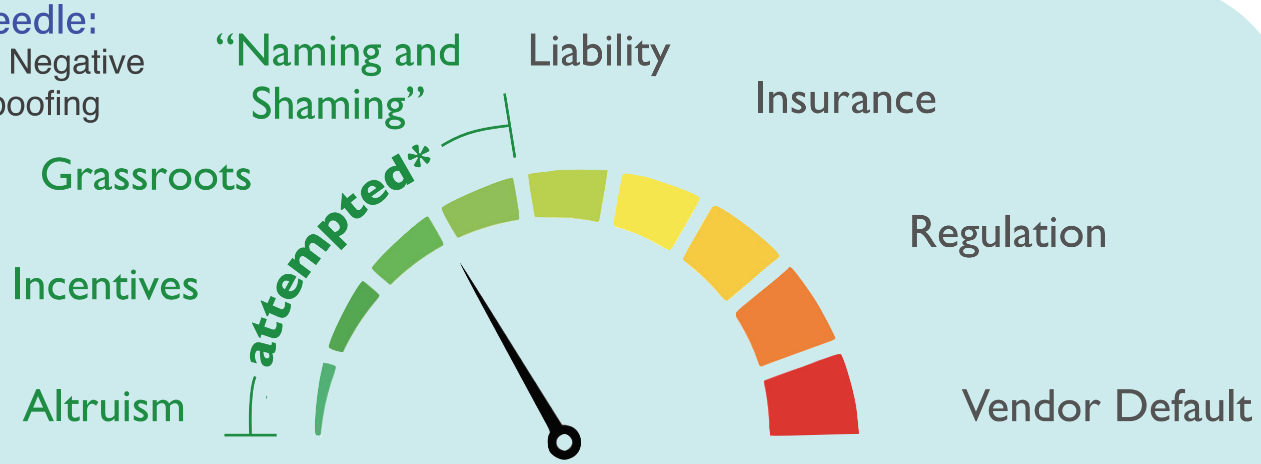
Spoofer measurement platform plays critical role

- quantifying current attack surface
- enabling third-party verification of deployment of SAV best practices,
- supporting assessment of the effectiveness of interventions (e.g., regulatory,

See ACM CCS 2019 paper for detailed policy analysis.*

Moving the Needle:

Internalizing the Negative Externality of Spoofing



*http://www.caida.org/publications/papers/2019/network_hygiene_incentives_regulation

Protect your network by downloading Spoofer measurement tool at: https://spoofer.caida.org

UC San Diego

SDSC SAN DIEGO SUPERCOMPUTER CENTER

caida

BCP 38