# SAVing the Internet – Methodologies to Detect Source Address Validation (SAV) by Network Providers

Qasim Lone[1] Mobin Javed [2] Maciej Korczyński[1] Hadi Asghari[1]
Matthew Luckie[3] Michel van Eeten[1]

[1] Delft University of Technology, the Netherlands

[2] University of California, Berkeley, USA

[3] University of Waikato, New Zealand

November 15, 2021

# What is IP Spoofing?

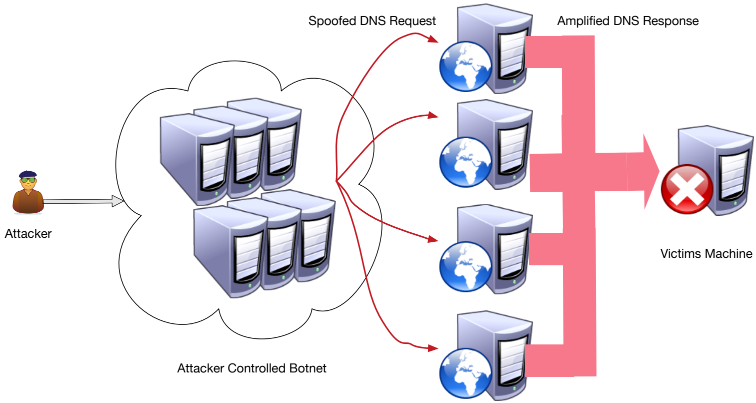
# What is IP Spoofing?

Using a forged IP address as the source address of a packet

# What is IP Spoofing?

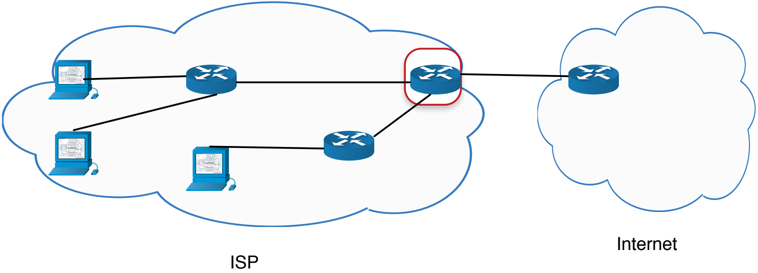
Using a forged IP address as the source address of a packet

Why spoof packets?



# How can we prevent IP spoofing ?

- At edge router of ISP:



# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?

# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?
- Why would network operators not filter spoofed packets?

# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?
- Why would network operators not filter spoofed packets?
- How do we know which operators have (or do not have) anti-spoofing measures in place?

# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?
- Why would network operators not filter spoofed packets?
- How do we know which operators have (or do not have) anti-spoofing measures in place?
    - Traceroute Loops (Misconfiguration of routers)

# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?
- Why would network operators not filter spoofed packets?
- How do we know which operators have (or do not have) anti-spoofing measures in place?
  - Traceroute Loops (Misconfiguration of routers)
  - IXP based methods

# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?
- Why would network operators not filter spoofed packets?
- How do we know which operators have (or do not have) anti-spoofing measures in place?
    - Traceroute Loops (Misconfiguration of routers)
    - IXP based methods
    - Open Resolver (Misconfiguration of certain CPEs)

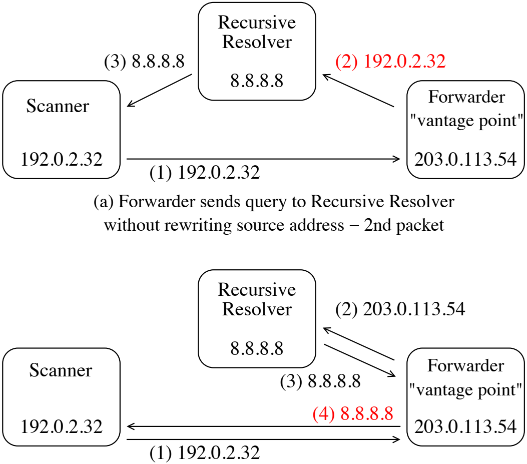
# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?
- Why would network operators not filter spoofed packets?
- How do we know which operators have (or do not have) anti-spoofing measures in place?
    - Traceroute Loops (Misconfiguration of routers)
    - IXP based methods
    - Open Resolver (Misconfiguration of certain CPEs)
    - Spoofer project (Client-server application)

# How can operators prevent IP spoofing?

- How can we prevent malicious users sending spoofed packets?
- Why would network operators not filter spoofed packets?
- How do we know which operators have (or do not have) anti-spoofing measures in place?
  - Traceroute Loops (Misconfiguration of routers)
  - IXP based methods
  - Open Resolver (Misconfiguration of certain CPEs)
  - Spoofer project (Client-server application)

# Open-resolvers based methodology



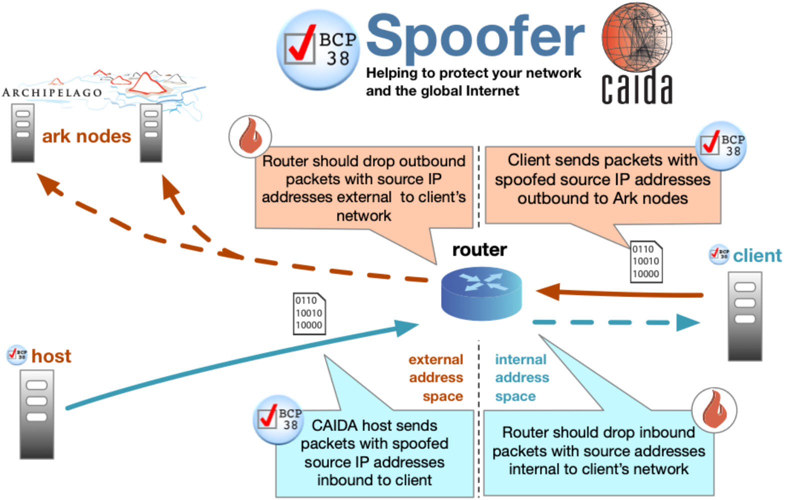
(a) Forwarder sends query to Recursive Resolver
without rewriting source address – 2nd packet

(b) Forwarder sends reply to Scanner
without rewriting source address – 4th packet

# Results of open-resolver based scans

- We performed Internet-wide forwarders-based scans of IPv4space weekly between September 2020 and February 2021
- We found 2,433 ASes operated by 2,320 providers as being non-compliant
- We find these providers in 118 countries

# Spoofer Tool



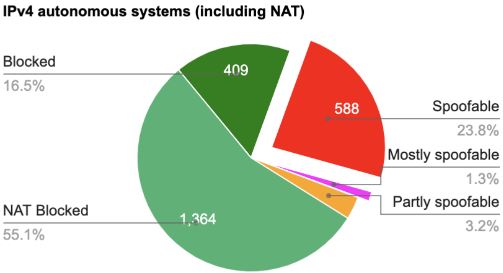
Router should drop outbound packets with source IP addresses external to client's network

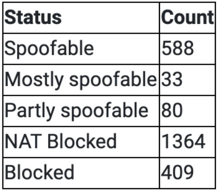
Client sends packets with spoofed source IP addresses outbound to Ark nodes

CAIDA host sends packets with spoofed source IP addresses inbound to client

Router should drop inbound packets with source addresses internal to client's network

# Spoofer Tool





| Status | Count |
|---|---|
| Spoofable | 588 |
| Mostly spoofable | 33 |
| Partly spoofable | 80 |
| NAT Blocked | 1364 |
| Blocked | 409 |

# Crowd sourcing Marketplaces to conduct Internet research

# Crowd sourcing marketplaces to conduct Internet research

As an alternative, we can collect additional data points using crowd sourcing platforms

- These platforms allows requesters to hire Internet workers to participate in simple jobs requiring few minutes to complete
- Participants can select jobs and earn ranging from few cents to few dollars per job

  Some examples of type of jobs posted are:

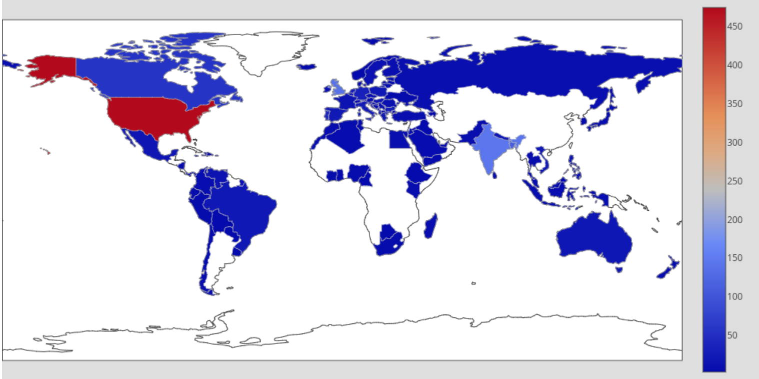
  - Tagging of pictures to train Artificial Intelligence algorithms
  - Survey of new products
  - Translation of text

# Selection of platforms to run Spoofer application

We selected following five platforms and requested participants to download and run Spoofer application to earn

| **Platform** | **Geographic Coverage** |
|---|---|
| Amazon Turk | US and IN |
| ProA | UK, US and diverse from EU |
| RapidWorkers | India, Bangladesh and US |
| Jobboy | US and Bangaldesh |
| Minijobz | Bangladesh, India Morocco |

# Coverage of crowdsourcing marketplaces



- Users successfully submitted Spoofer test results from 91 countries
- More than 1500 unique IPs tested in 6 weeks of study.
- Collected data from more than 700 unique ASes

# Results from Crowdsourcing measurements

- Using CAIDA's Spoofer tool we were able to acquire vantage points in 91 countries and 784 ASNs, 342 of which did not have a vantage point in the 12 months before our study
- We find evidence that measurement tasks are quite price sensitive and that higher compensation is likely to recruit even more vantage points.

# References

[1] Marc Kührer, Thomas Hupperich, Christian Rossow, and Thorsten Holz. **"Exit from hell? Reducing the impact of amplification DDoS attacks."** In 23rd USENIX Security Symposium (USENIX Security 14), pp. 111-125. 2014.
[2] Qasim Lone, Maciej Korczyński, Carlos Gañán, and Michel van Eeten. **"SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers."** In Workshop on the Economics of Information Security. 2020.
[3] Qasim Lone, Matthew Luckie, Maciej Korczyński, Hadi Asghari, Mobin Javed, and Michel Van Eeten. **"Using crowdsourcing marketplaces for network measurements: The case of spoofer."** In 2018 Network Traffic Measurement and Analysis Conference (TMA), pp. 1-8. IEEE, 2018