Behind Closed Doors:

A Network Tale of Spoofing, Intrusion, and False DNS Security

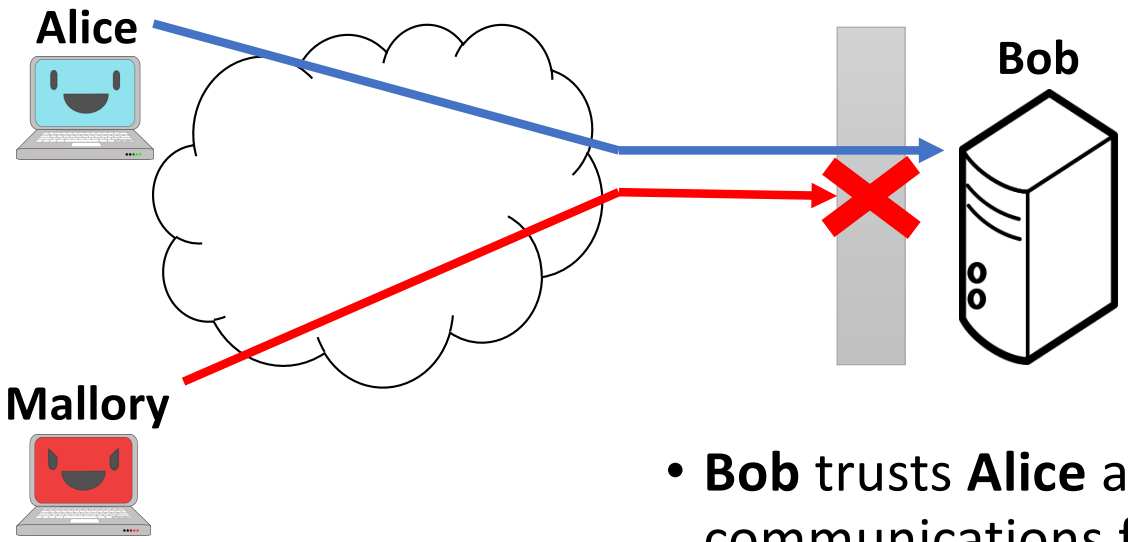
Casey Deccio, Alden Hilton,

Michael Briggs, Trevin Avery, Robert Richardson

Brigham Young University

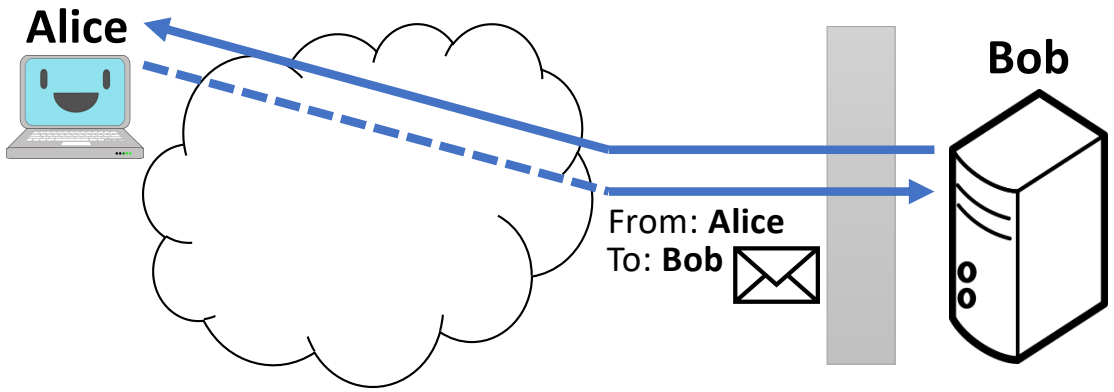
OARC 35

Access Control



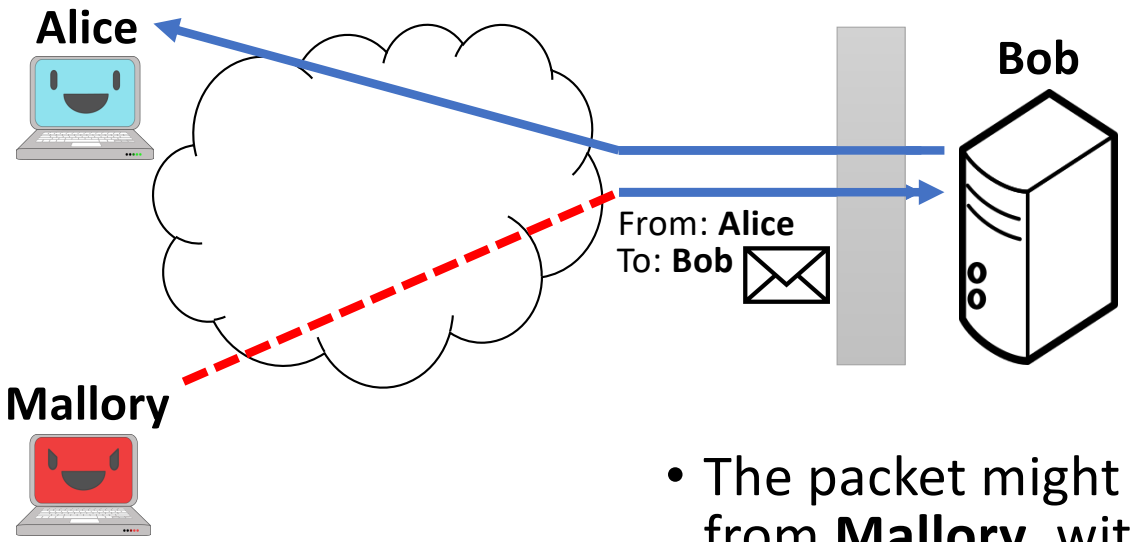
- **Bob** trusts **Alice** and *allows* communications from her
- **Bob** does not trust **Mallory** and *blocks* communications from her.

The Problem: Internet Identity



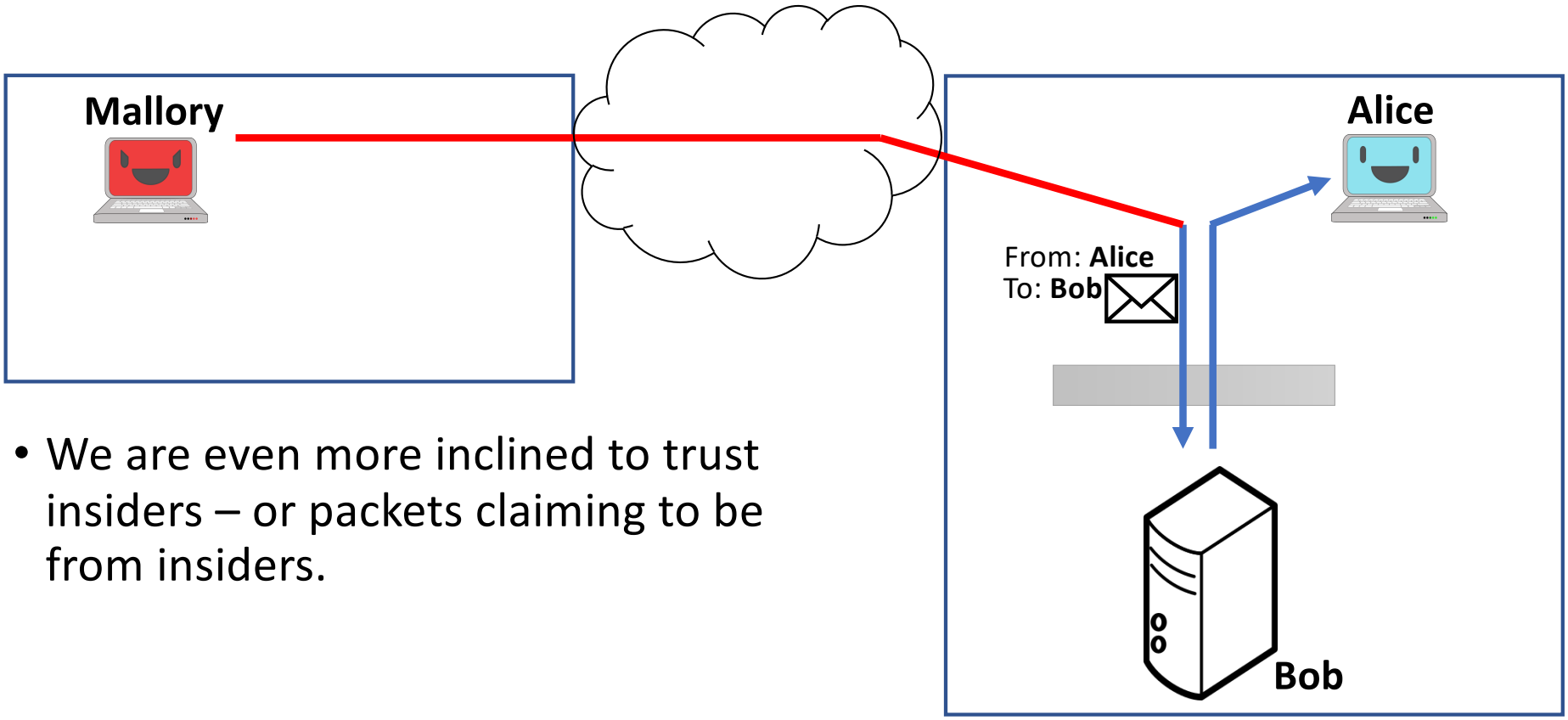
- Should **Bob** trust a packet that claims to be from **Alice**?

The Problem: Internet Identity



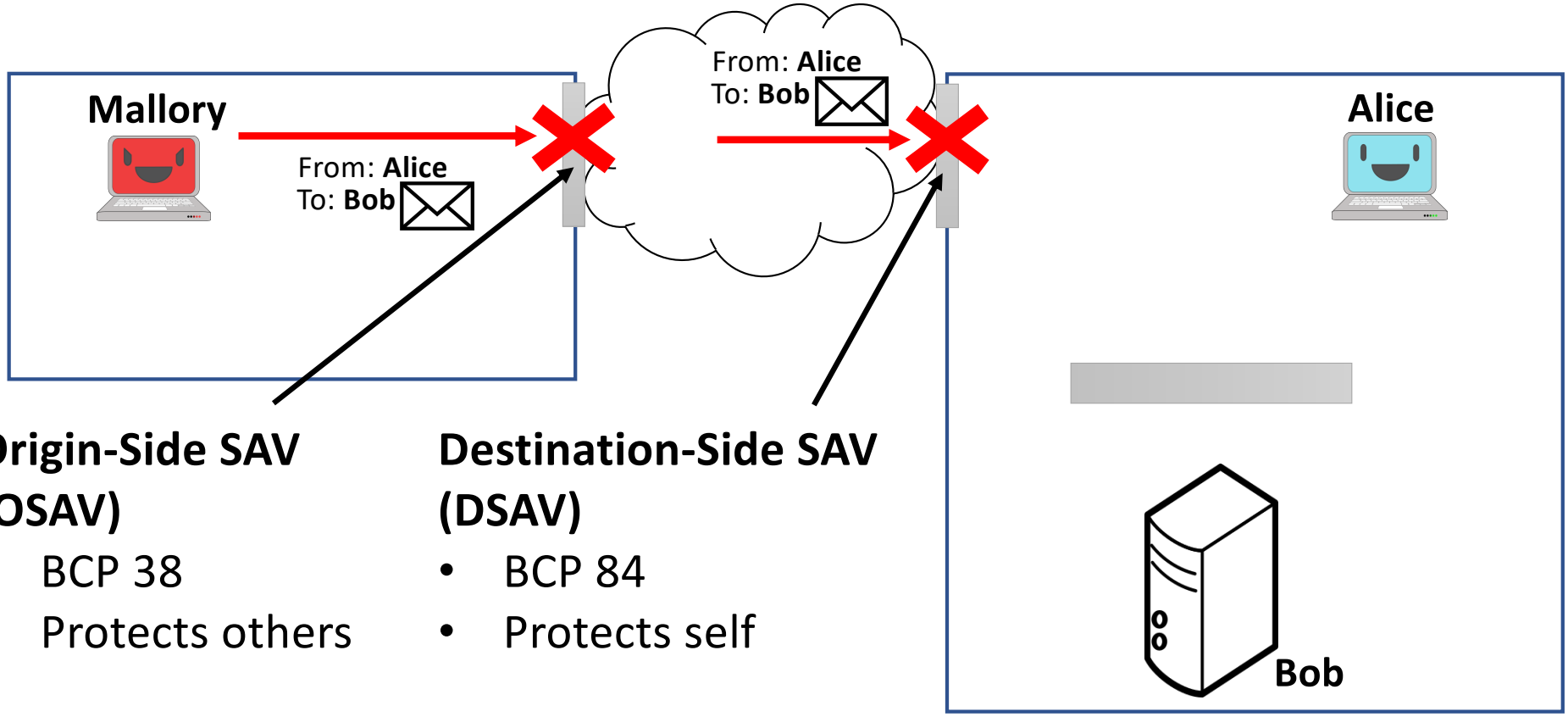
- The packet might have originated from **Mallory**, with spoofed source!
- The response constitutes ***reflection***

Insider Trust



- We are even more inclined to trust insiders – or packets claiming to be from insiders.

Source Address Validation (SAV)



Origin-Side SAV (OSAV)

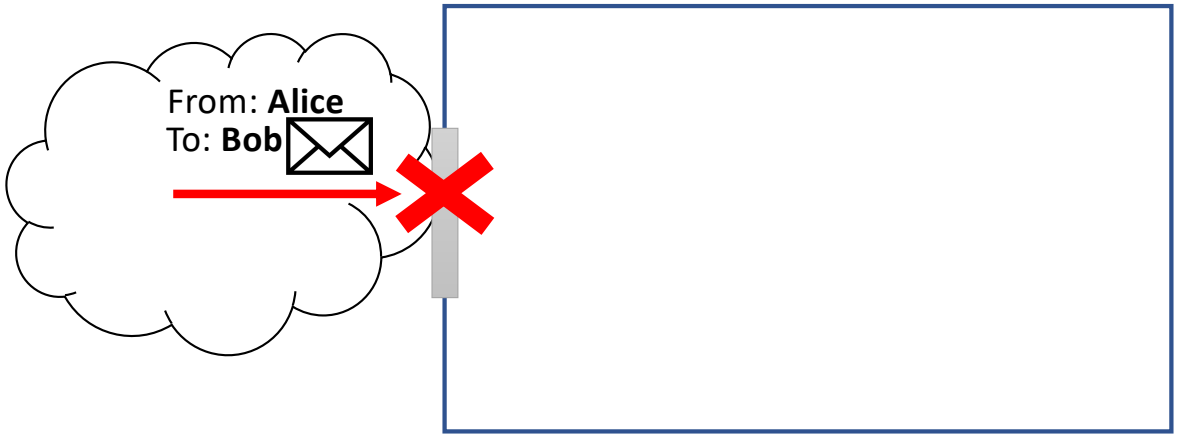
- BCP 38
- Protects others

Destination-Side SAV (DSAV)

- BCP 84
- Protects self

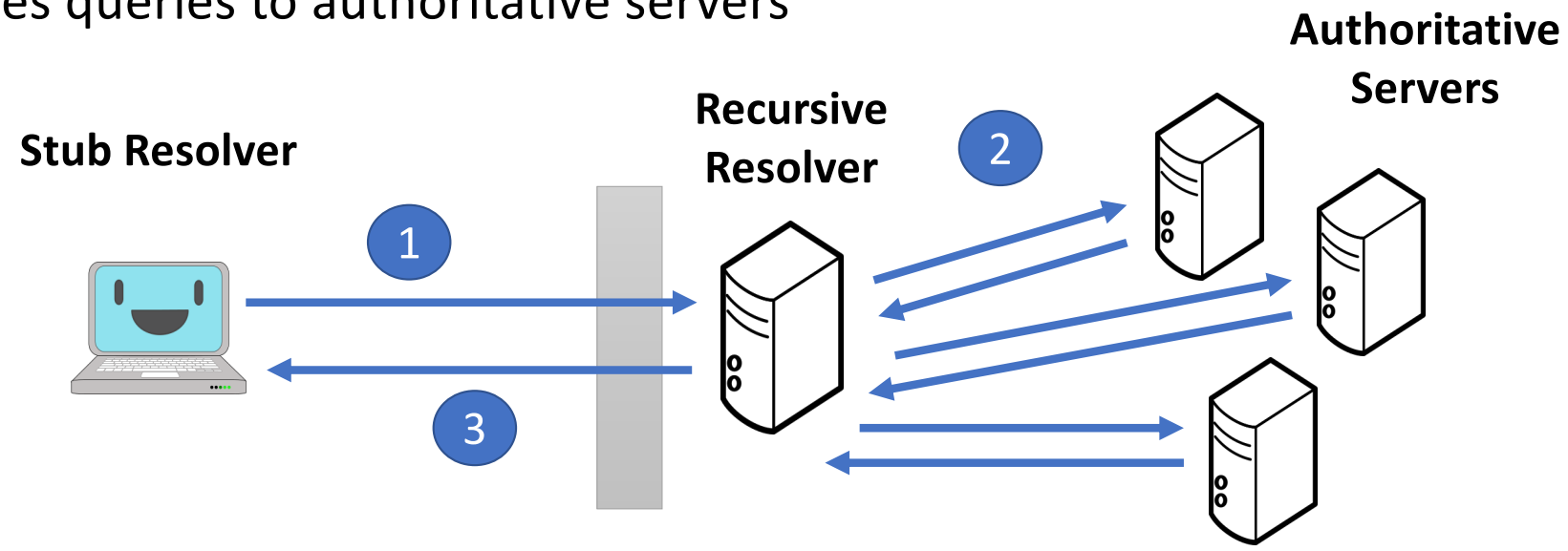
Research Question

- How prevalent is destination-side source address validation (DSAV)?

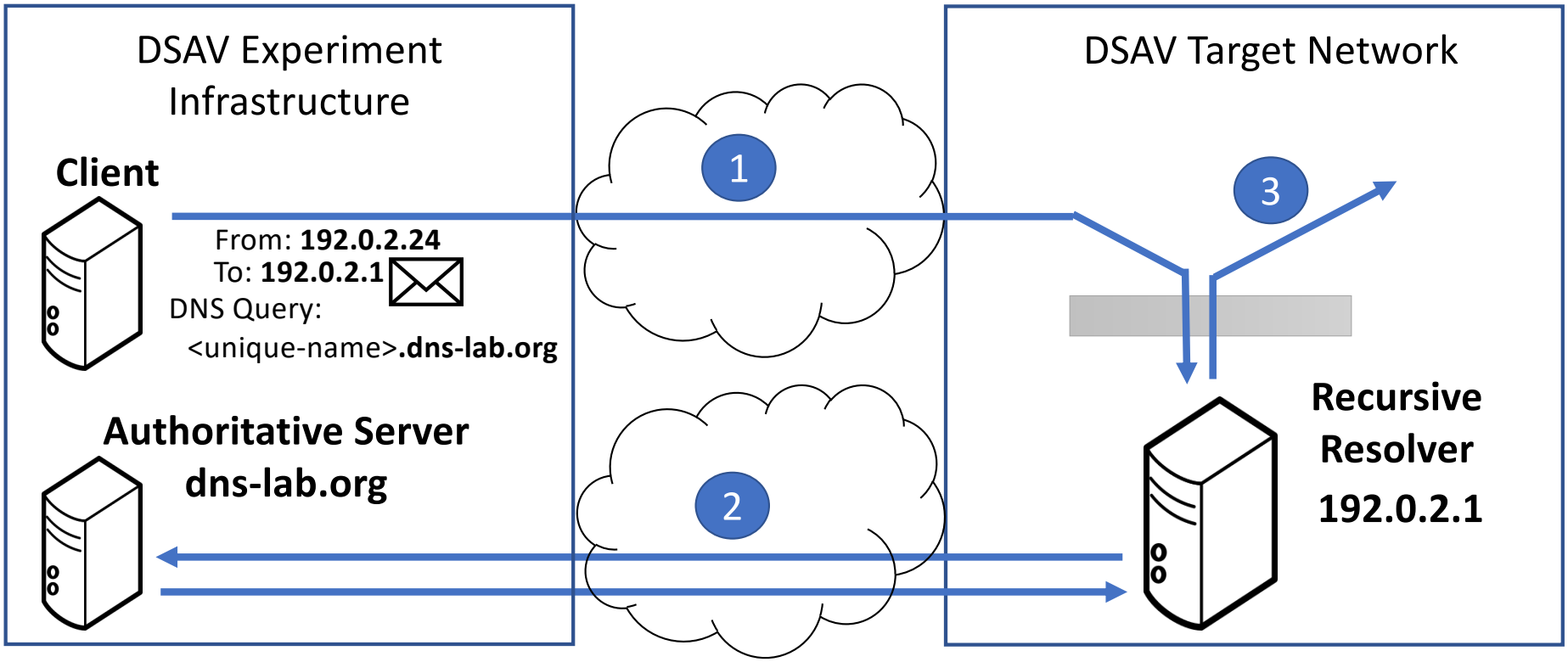


Domain Name System (DNS)

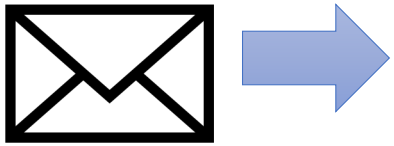
- Primary query/response transport is UDP
- Query requires only one (UDP) packet
- One trusted packet at recursive resolver forces queries to authoritative servers



The Experiment: Measure DSAV Using the DNS



The Experiment: Destinations and Sources



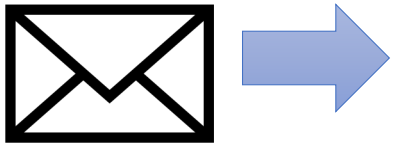
Spoofed Sources

- **Other Prefix** – Up to 97 addresses, from distinct /24 or /64 prefixes announced by the same AS
- **Same Prefix** – 1 address from same /24 or /64 prefix
- **Private** – 192.168.0.10 or fc00::10
- **Dest-as-Source –** Destination address itself
- **Loopback** – 127.0.0.1 or ::1

Target Destinations

- DNS clients from 48 hours of root server queries – April 2019
- IPv4:
  - ~11.2M IPv4 Addresses
  - ~54K IPv4 ASes
- IPv6:
  - ~800K IPv6 Addresses
  - ~8K IPv6 ASes

Experiment Results: Destinations and Sources



Source Effectiveness

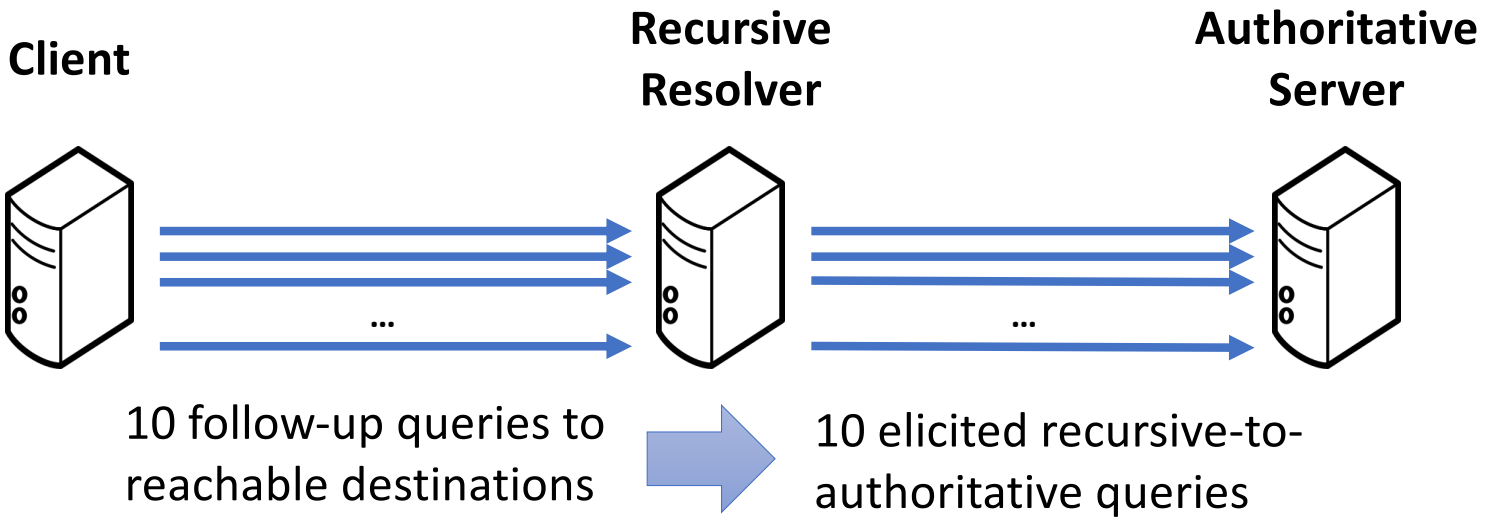
- **63%** and **84%** of reachable IPv4 and IPv6 targets reached by **same-prefix** sources
- **70%** of reachable IPv6 addresses reachable by **dest-as-source** source
- Targets *exclusively* reachable by sources:

	IPv4 Addresses	IPv6 Addresses
Other Prefix	**33%**	**4.9%**
Same Prefix	**17%**	**8.1%**
Private	**0.5%**	**0.5%**
Dest-as-Source	**2.6%**	**9.9%**
Loopback	**0**	**22**

Target Reachability

- IPv4
  - **4.6%** of destination addresses received query
  - **49%** of destination ASes included a responsive IPv4 address
- IPv6
  - **6.2%** of destination addresses received query
  - **50%** of destination ASes included a responsive IPv6 address

DNS Resolver Characterization



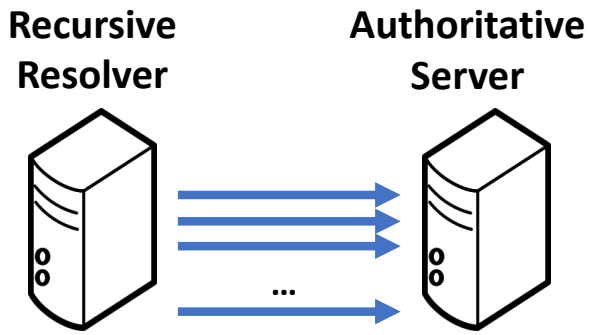
Computing Source Port Ranges From Recursive-to-Authoritative Queries

(Using only five ports as a simplified example.)

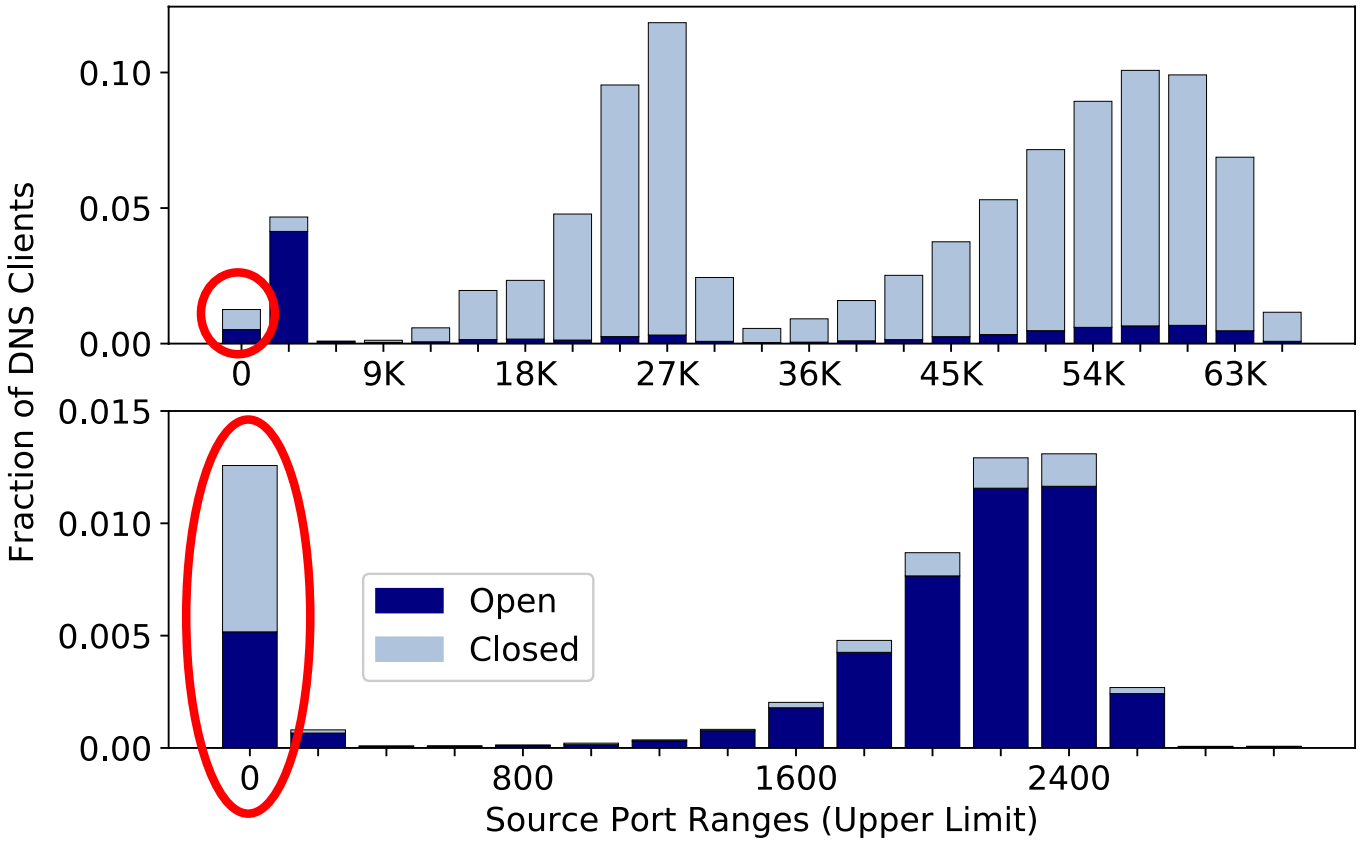
Raw list of source ports: 25 16 60 70 15

Sorted list of source ports: 15 16 25 60 70

Range of source ports: 70 – 15 = 55



Distribution of Observed Source Port Ranges



Ranges 0 through 65535

Ranges 0 through 3000

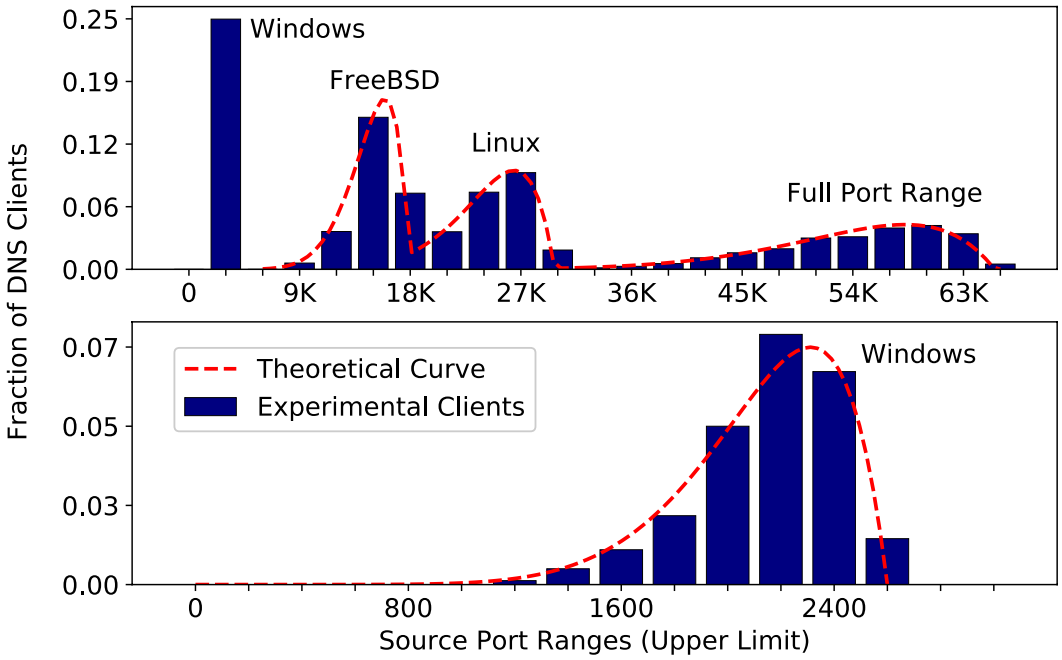
DNS Resolver Characterization: Zero-Range Source Ports

- Affected resolvers: **3,810**
- Problem: more vulnerable to **cache poisoning** (Kaminsky 2008)
- Possible causes:
  - **old software** (BIND 8, Windows DNS pre-2008 R2)
  - **outdated configurations** ("query-source address * port 53")
- Most common source ports: **53** (34%), **32768** (12%), **32769** (3.8%)
- Comparison to 48 hours of root queries – April 2018
  - 51% of vulnerable resolvers **lacked source-port randomization** in 2018
  - 25% of vulnerable resolvers **used random source ports** in 2018

OS Fingerprinting Using Source Port Ranges: Lab Experiment

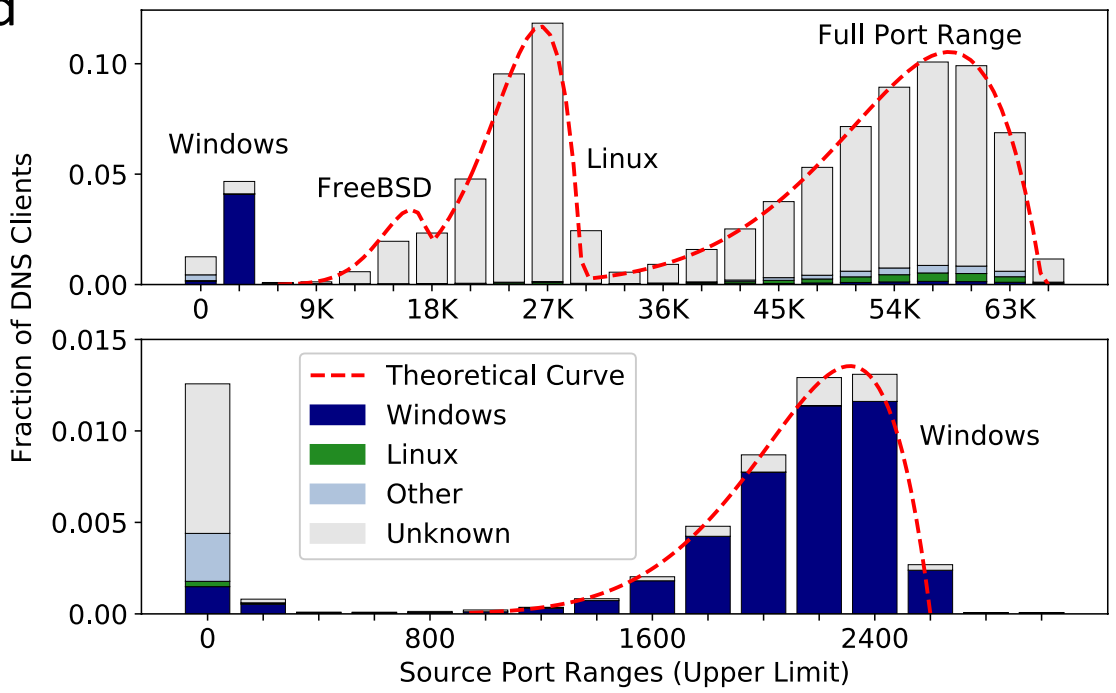
- Issued 1,000 sets of 10 queries in a lab environment
  - BIND 9.11 on **FreeBSD**
  - BIND 9.11 on **Linux 2.6 – 5.3**
  - **Windows DNS 2008 R2 – 2019**
- Source port ranges follow a Beta distribution:

  $Beta(\alpha, \beta), \alpha = 9, \beta = 2$



OS Fingerprinting Using Source Port Ranges: **Target Resolver Data**

- p0f OS fingerprinting tool used to validate our findings
- **89%** of machines identified as Windows **supported by p0f**
- **89%** of machines identified as Windows identified as **open resolvers**

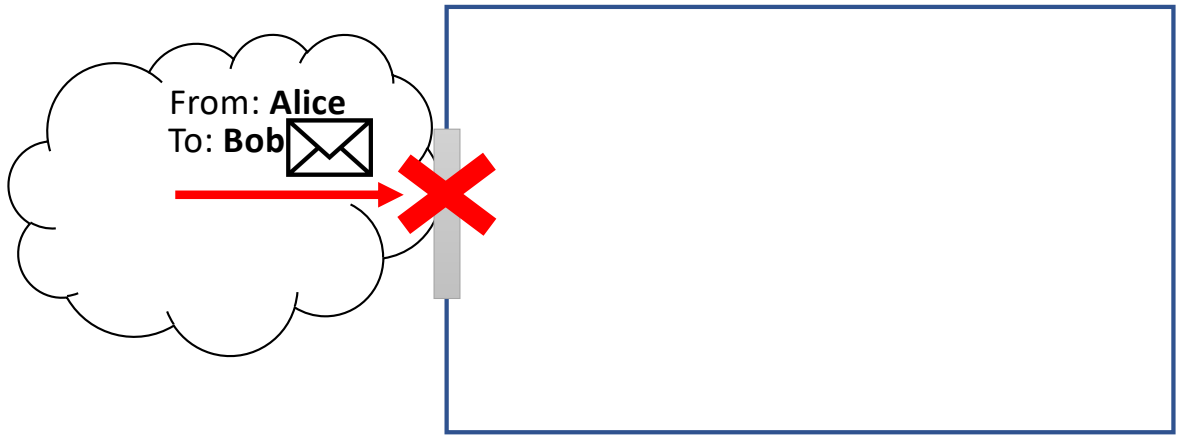


Spoofing Allowed By OS: Lab Experiment

OS	Linux Kernel	IPv4		IPv6	
		Dest-as-Source	Loopback	Dest-as-Source	Loopback
Ubuntu 16.04, 18.04, 19.04	4.15, 5.3, 5.0			●	
Ubuntu 10.04, 12.04, 14.04	2.6, 3.13, 4.4			●	●
FreeBSD 12.1, 12.0, 11.3		●		●	
Windows Server 2008, 2008 R2 2012, 2012 R2,2016, 2019		●		●	
Windows Server 2003, 2003 R2		●	●	●	

Summary

- The source address of network packets cannot be trusted.
- Source address validation should be implemented at both the origin (OSAV) and the destination (DSAV).
- DSAV is found to be lacking in half of measured networks.



Reach-Out and Test Tool

- Individual reach-out
  - Looked up contact information for the ~25K ASes identified by our research
  - Sent email with an individualized report and self-test tool to every contact
  - Response analysis is pending, but response was *generally* positive
- Self-test tool:

  https://dsav-test.byu.edu/ => TRY IT!!

Previous Work

- OSAV/BCP38 Measurement (Spoofer Project)
  - [Beverly, IMC 2009]
  - [Luckie, CCS 2019]
- DSAV Measurement
  - [Korczyński, PAM 2020]
- Internal Resolver Analysis
  - [Scheffler, PAM 2018]

Contact Information

Please send questions and comments to:

dsav-info@byu.edu

All images are public domain, obtained from openclipart.org