Software Systems for Surveying Spoofing Susceptibility
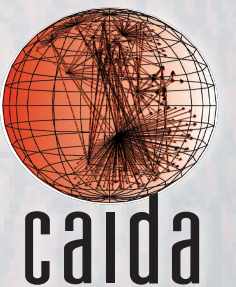
Matthew Luckie, Ken Keys, Ryan Koga,
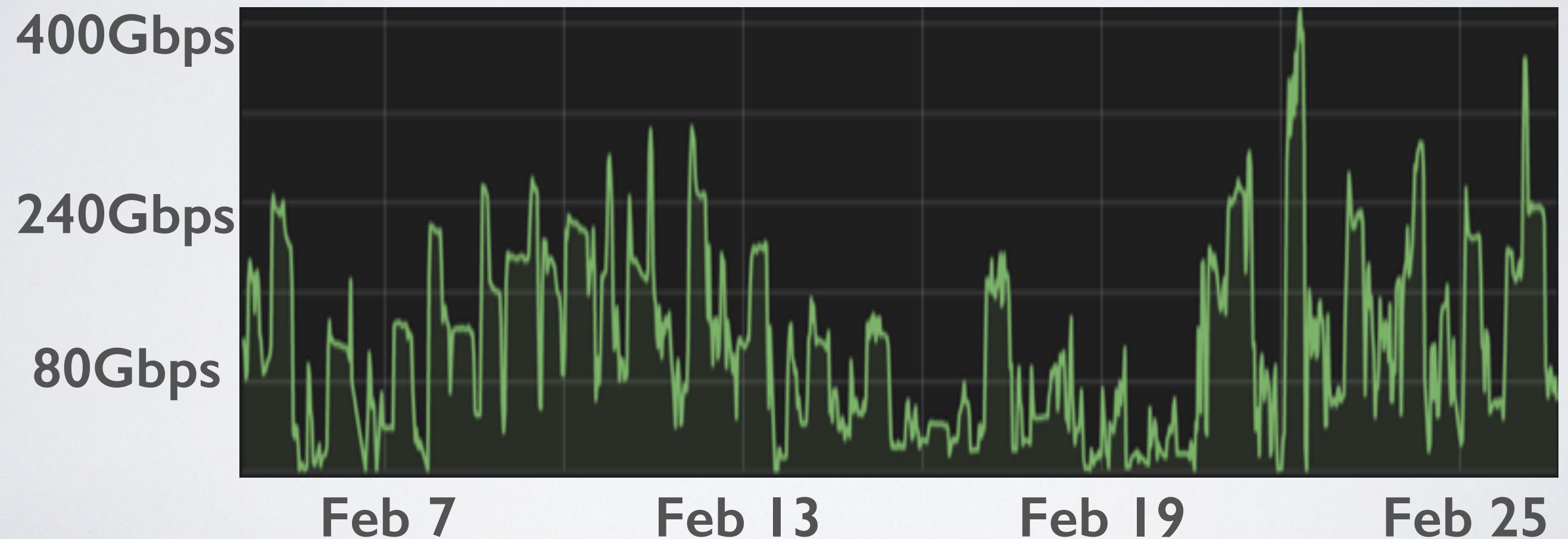Bradley Huffaker, Robert Beverly, *kc claffy*

## https://spoofer.caida.org/

NANOG68, October 18th 2016

What is the Problem?

- Lack of **anti-spoofing filtering** allows anonymous denial of service attacks.

- Example: CloudFlare reports **400Gbps attacks** on their systems through 2016

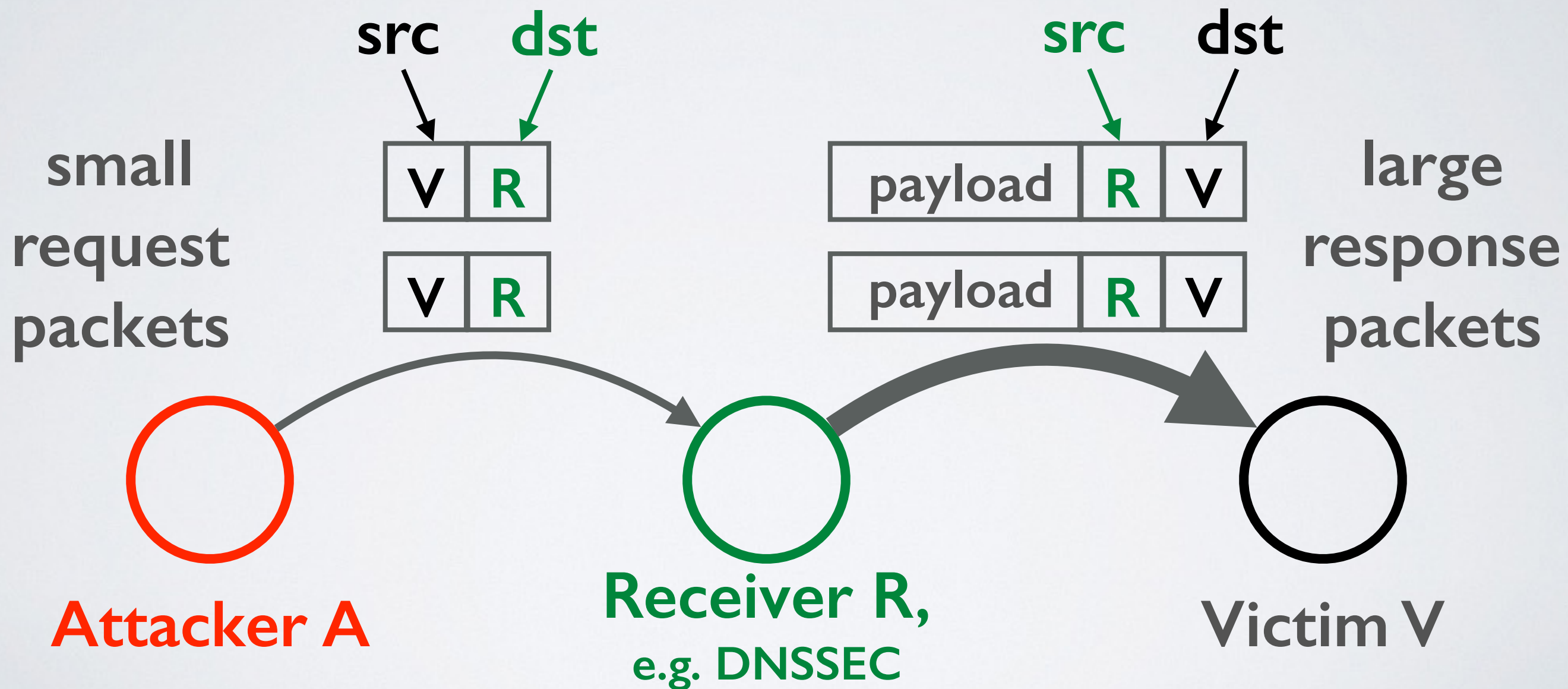https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/

What is the Problem?

- Lack of *anti-spoofing* filtering allows anonymous DoS attacks.

- Example: CloudFlare reports **>1K DoS attack events** on their systems, per day, starting **Feb 2016**

https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/
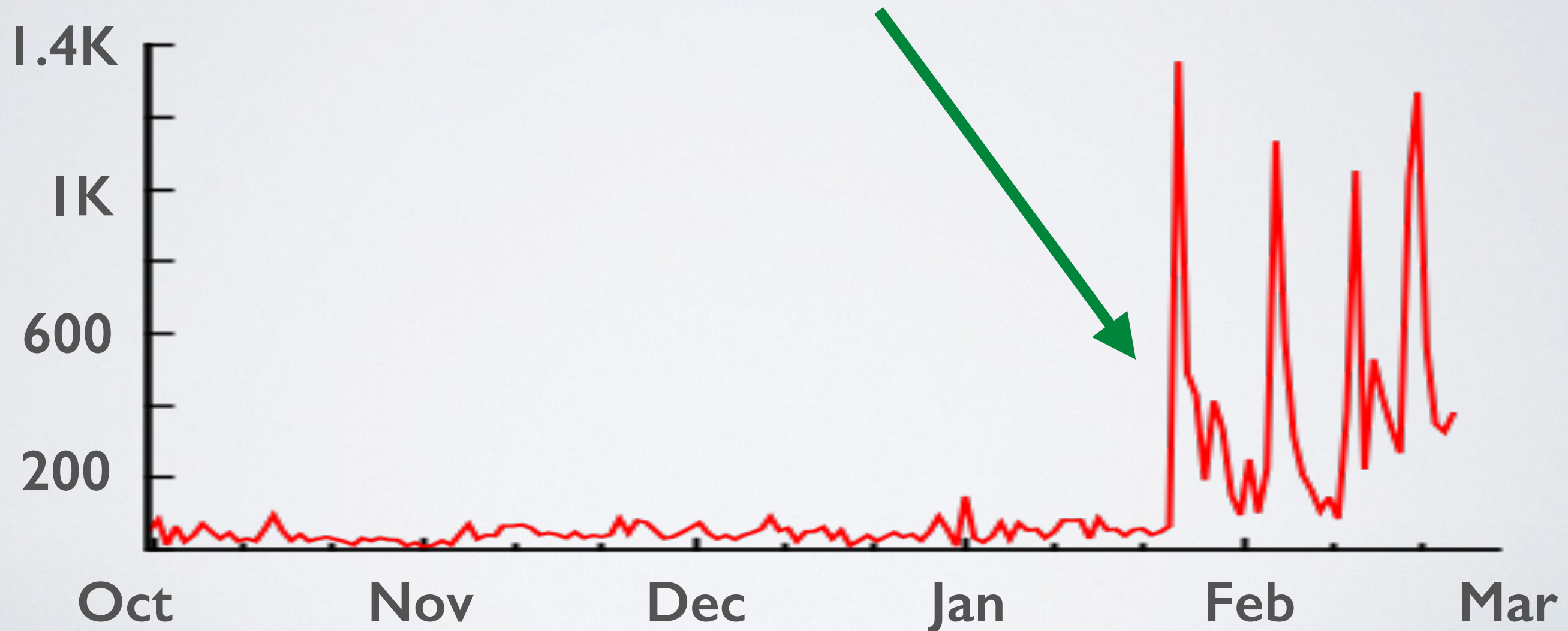
Why does spoofing matter?

- Attacker sends packet with spoofed source IP address

- Receiver cannot generally know if packet's source is authentic

small request packets

src **dst**

| V | R |
| V | R |

large response packets

src **dst**

| payload | R | V |
| payload | R | V |

Attacker A

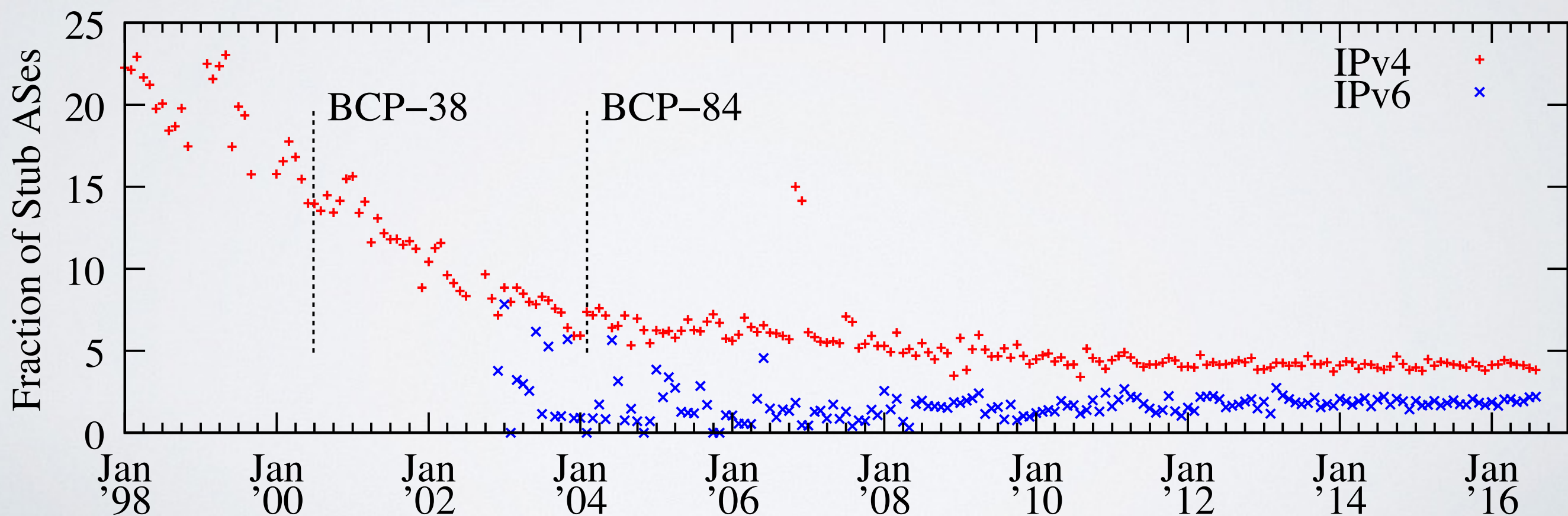**Receiver R,** e.g. DNSSEC

Victim V

Volumetric Reflection-Amplification Attack

Defenses

- **BCP38**: Network ingress filtering: defeating denial of service attacks which employ IP Source Address Spoofing

  - https://tools.ietf.org/html/bcp38

  - May 2000

- **BCP84**: Ingress filtering for multi-homed networks

  - https://tools.ietf.org/html/bcp84

  - March 2004

- Not always straightforward to deploy "*source address validation*" (SAV): BCP84 provides advice how to deploy

Use Ingress Access Lists!

ACLs are "the most bulletproof solution when done properly", and the "best fit ... when the configuration is not too dynamic, .. if the number of used prefixes is low". - BCP84

During 2015, ~5% and ~3% of ASes announced different IPv4 and IPv6 address space month-to-month, respectively.
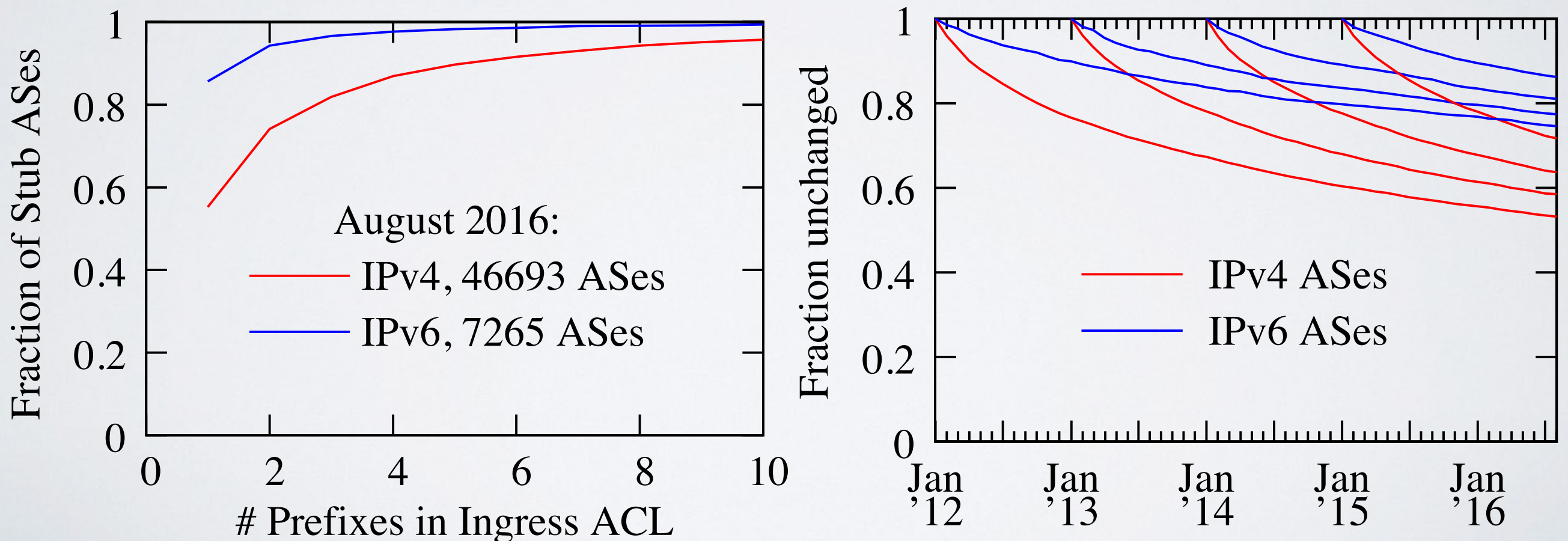
Use Ingress Access Lists!

ACLs are the "best fit ... when the configuration is not too dynamic, .. if the number of used prefixes is low". - BCP84

In August 2016, 86.9% of stub ASes would require an IPv4 ACL of no more than 4 prefixes. More than half of IPv4 ACLs defined in January 2012 would still be unchanged today.

August 2016:
— IPv4, 46693 ASes
— IPv6, 7265 ASes

(Left plot axes) Fraction of Stub ASes vs # Prefixes in Ingress ACL

IPv4 ASes
IPv6 ASes

(Right plot axes) Fraction unchanged vs Jan '12, Jan '13, Jan '14, Jan '15, Jan '16

Source Routeviews and RIPE RIS data

Tragedy of the Commons

- Deploying source address validation is **primarily for the benefit of other networks**

- **Incentive not clear for some networks**

  - majority of networks do seem to deploy filtering

  - filtering gives an operator moral high-ground to pressure other networks to deploy, which does benefit the operator

  - "Cyber Insurance" takes into account security practice of the network: QuadMetrics.com

- ISOC RoutingManifesto.org: Mutually Agreed Norms for Routing Security (MANRS)

M A N R S

Which networks have deployed filtering?

- **No public data that allows a network to show that they have (or have not) deployed filtering**

- **OpenResolverProject**: allows detection of which networks have not deployed filtering based on DNS request forwarding

  - requires a buggy open resolver

  - public reporting at network and AS level

- **MIT/CMAND Spoofer Project**: aggregated statistics of spoofability based on crowd-sourced tests

  - user had to manually run tests

  - no public reporting at network or AS level

Spoofer: Client/Server Overview

TCP control connection

Client

Spoofer Server

Spoofed packets

Database

CAIDA Ark Vantage Points
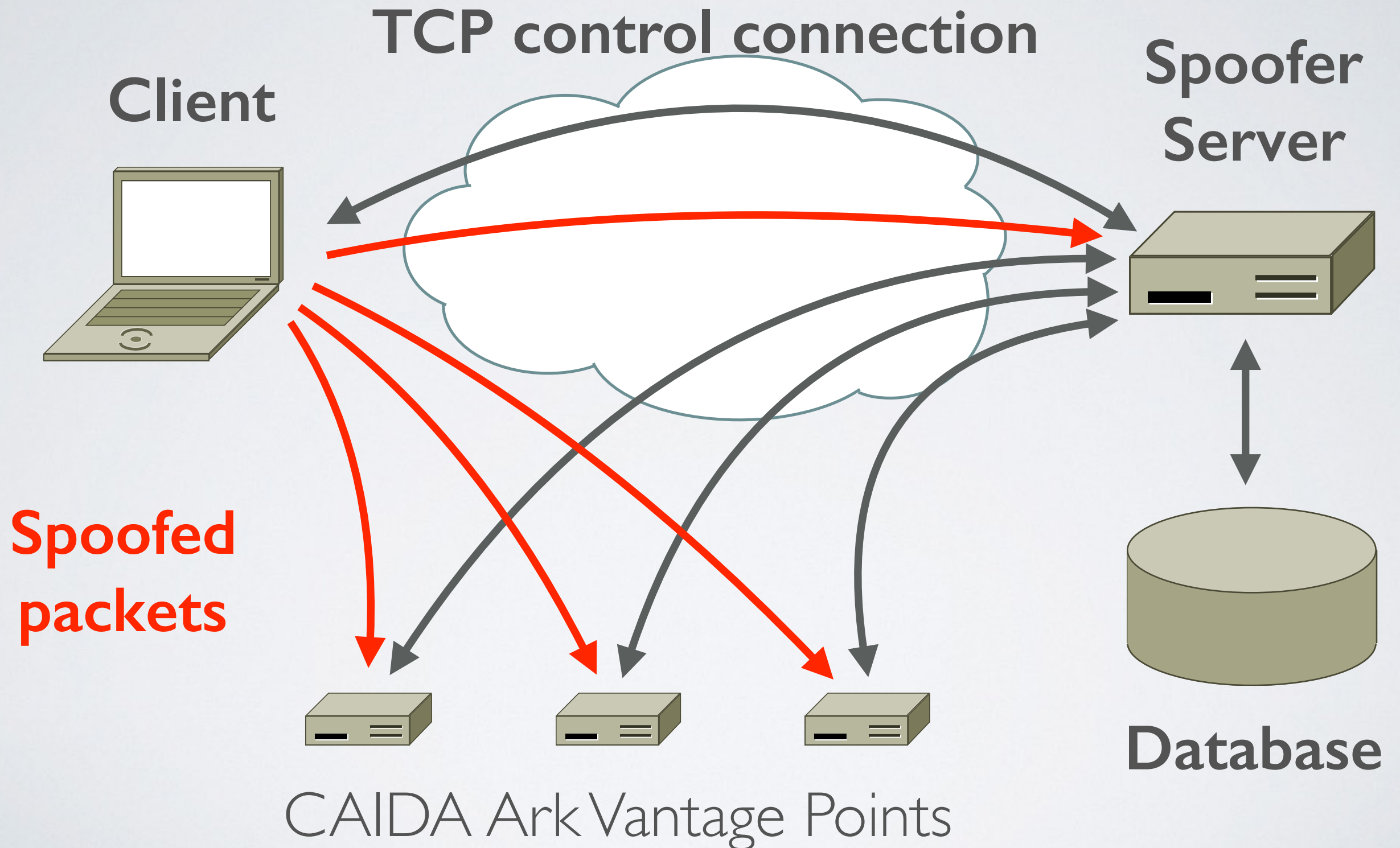
Spoofer: Client/Server Overview

- Client tests ability to spoof packets of different types

  - Routed and Private

  - IPv4 and IPv6

- **`traceroute`** to infer forward path to destinations

- **`tracefilter`** to infer first location of filtering in a path

  - traceroute but with spoofed packets

- Filtering prefix granularity: how many addresses in the same network prefix can be spoofed?

CAIDA Spoofer Project: New Features

- **Client/Server** system provides new useful features

  - **by default: publicly share anonymized results**

  - **by default: share unanonymized results for remediation**

  - Runs in background, automatically testing new networks the host is attached to, once per week, IPv4 and IPv6

  - GUI to browse test results from your host, schedule tests

- **Reporting Engine** publicly shows outcomes of sharable tests

  - Allows users to select outcomes per country, per ASN

  - **https://spoofer.caida.org/recent_tests.php**

CAIDA Spoofer Project: Ethical Issues

- Unlike measurement of DNSSEC, IPv6, etc, measurement of spoofing requires spoofing from vantage point in the network

  - We see no other way to approach this problem

  - Other methods can provide limited complementary coverage, but not under a user's control

  - Running it once: limited coverage, representativeness

  - Debates over years about appropriate level of transparency

- We send spoofed packets **slowly** to **machines we control**

- We see operators using it for remediation

Client GUI

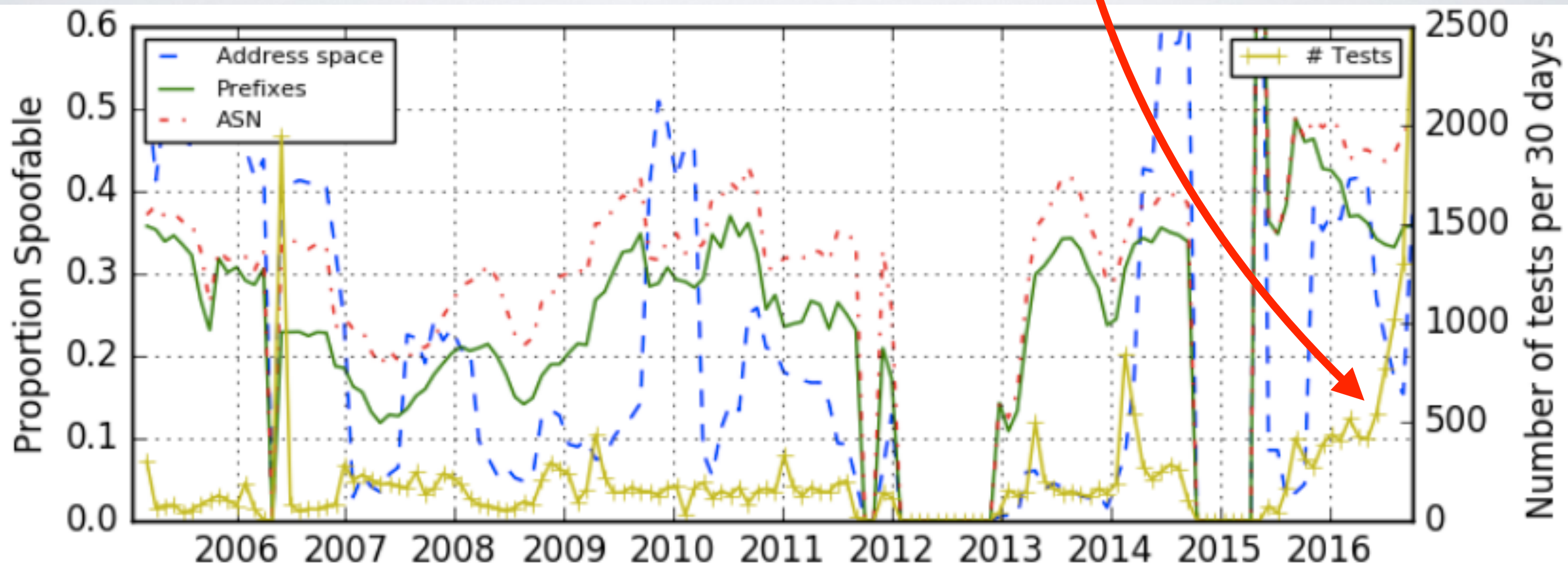## (https://spoofer.caida.org/)

Signed Installers
MacOS
Windows
Linux

Open Source
C++

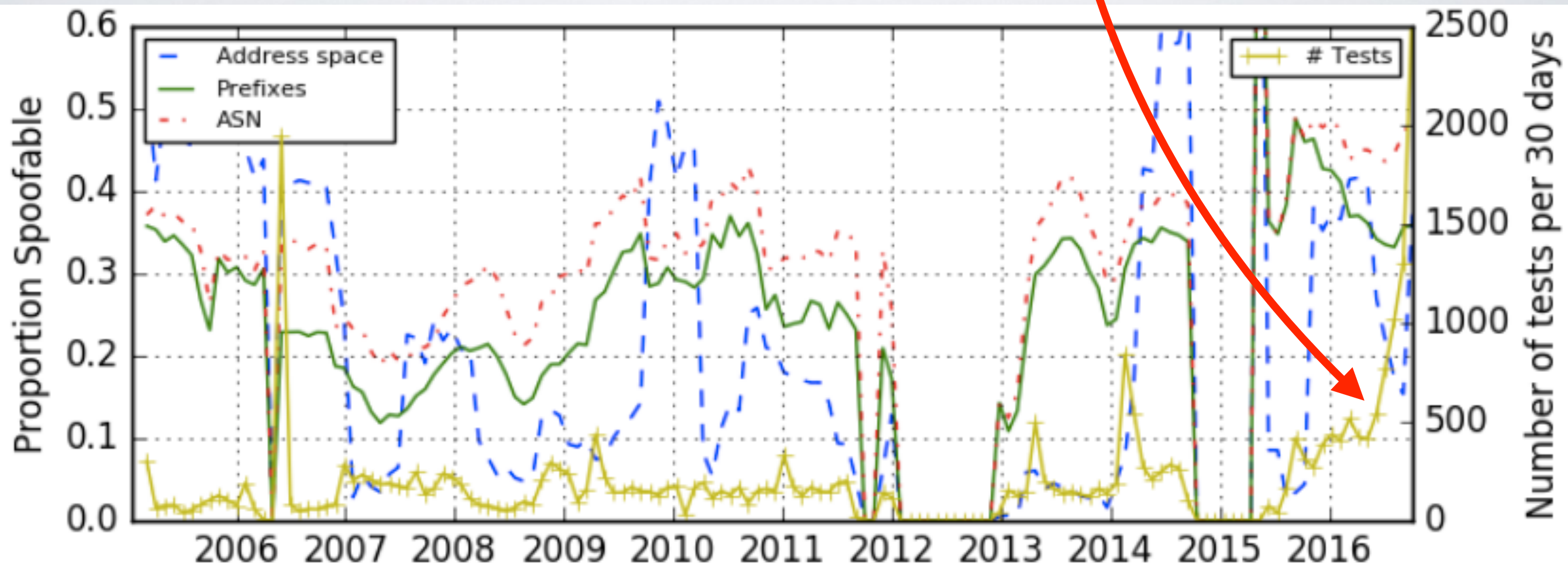# Client/Server Deployment

- Since releasing new client in May, increasing trend of more tests (yellow line)

  - Benefit of system running in background

Client/Server Deployment

- Since releasing new client in May, increasing trend of more tests (yellow line)

  - Benefit of system running in background

Reporting Engine: Recent Tests

Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306::x	7018		no	blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007::x	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106::x	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78402	2016-10-14 09:51:52	216.227.79.x	13673	usa	yes	blocked	blocked	none	Full report
78388	2016-10-14 08:52:15	216.47.128.x	29825	usa	no	unknown	unknown	none	Full report
		2620:f3::x	29825		no	unknown	unknown		
78385	2016-10-14 08:48:22	50.54.90.x	5650	usa	yes	blocked	blocked	none	Full report
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Reporting Engine: Recent Tests

Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14								Full report
78448	2016-10-14								Full report
78446	2016-10-14								Full report
78440	2016-10-14								Full report
78437	2016-10-14	2600:1007::x	22394		no	blocked	blocked		Full report
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106::x	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78402	2016-10-14 09:51:52	216.227.79.x	13673	usa	yes	blocked	blocked	none	Full report
78388	2016-10-14 08:52:15	216.47.128.x	29825	usa	no	unknown	unknown	none	Full report
		2620:f3::x	29825		no	unknown	unknown		
78385	2016-10-14 08:48:22	50.54.90.x	5650	usa	yes	blocked	blocked	none	Full report
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Able to break down by country, perhaps useful for regional CERTs.
In this case US-CERT

Reporting Engine: Recent Tests

Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306::x	7018		no	blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	31412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007::x	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106::x	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa					
78402	2016-10-14 09:51:52	216.227.79.x	13673	usa					
78388	2016-10-14 08:52:15	216.47.128.x	29825	usa					
		2620:f3::x	29825						
78385	2016-10-14 08:48:22	50.54.90.x	5650	usa					
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa					
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Addresses anonymized:
IPv4: /24
IPv6: /32 (thinking /40)

Reporting Engine: Recent Tests

Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306:x	7018			blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007::x	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106::x	11039		no	received	received		
78416	2016-								Full report
78402	2016-								Full report
78388	2016-								Full report
78385	2016-								Full report
78381	2016-								Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

NATs behave differently:
Some may block spoofed traffic
Some uselessly rewrite
Some do not rewrite and pass spoofed packets

Reporting Engine: Recent Tests

Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306::x	7018		no	blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007::x	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106::x	11039		no	received	received		
78416									Full report
78402									Full report
78388									Full report
78385									Full report
78381									Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Some networks may have deployed IPv4 filtering,
but forgotten to deploy IPv6 filtering

How can you help?

- **Install the client! (spoofer.caida.org)**

- Room full of laptops and people who travel (use different networks). Great opportunity to collect new users and grow visibility of filtering deployment practice

- What about NAT?

  - Not all NAT systems filter packets with spoofed source addresses

  - Roughly 35% of test results that showed spoof-ability were conducted from behind a NAT

Notifications and Remediation

- Currently, we (Matthew) manually send notifications to abuse contacts of prefixes from which we received spoofed packet

Successful filtering deployment: weekly tests show spoofed packets are now blocked

Session	Timestamp	Client IP	ASN	Country					
65845	2016-08-20 21:57:21	185.20.52.x	61049	gbr					
64872	2016-08-13 20:45:49	185.20.52.x	61049	gbr					
64108	2016-08-06 19:33:36	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
63277	2016-07-30 18:21:24	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
62416	2016-07-23 17:09:58	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
61733	2016-07-16 15:58:12	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
61078	2016-07-09 14:46:05	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
60453	2016-07-02 13:33:56	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
59702	2016-06-25 12:21:55	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
59596	2016-06-24 08:14:07	185.20.52.x	61049	gbr	no	received	received	/9	Full report
58866	2016-06-17 07:02:32	185.20.52.x	61049	gbr	no	received	received	/9	Full report
58224	2016-06-10 05:50:36	185.20.52.x	61049	gbr	no	received	received	/9	Full report
58220	2016-06-10 04:20:37	185.20.52.x	61049	gbr	no	received	received	/9	Full report

Traceroute-based inferences: Expanding View of Filtering Policy

- Use CAIDA traceroute data to infer customer-provider links to stub ASes that imply lack of ingress filtering by provider

- Goal: expand view of filtering policy, spur additional deployment of ingress ACLs

- Method suggested by Jared Mauch (NTT), joint work with Qasim Lone (TU Delft)

Provider #1

Provider #2

VP **S**

VP **S**

Stub AS

VP **S**
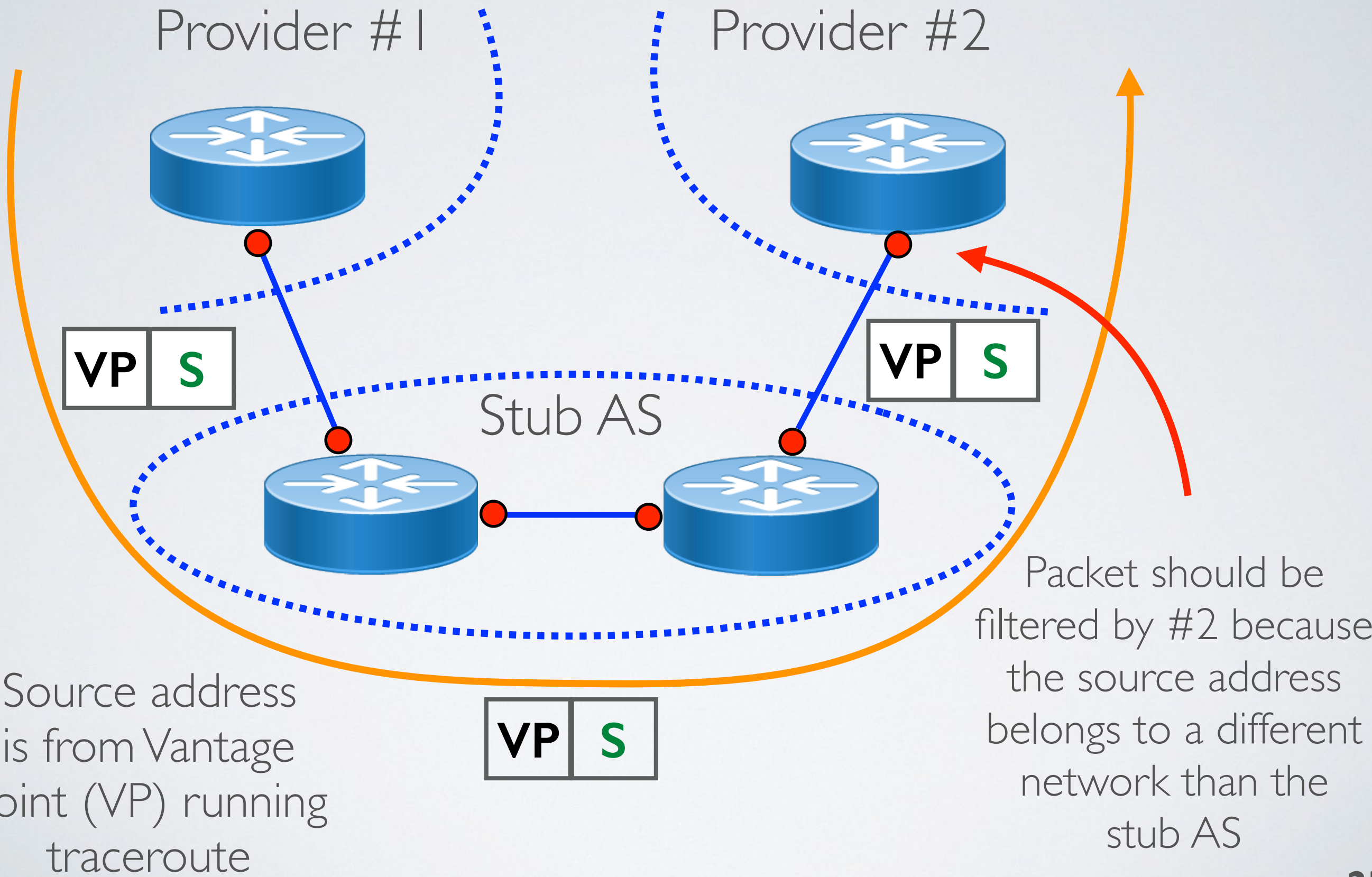
Source address is from Vantage Point (VP) running traceroute

Packet should be filtered by #2 because the source address belongs to a different network than the stub AS

Traceroute Spoofer: 3356-5088

```
12.83.46.1     7018
12.123.16.85   7018          gar26.dlstx.ip.att.net
4.68.62.229    3356_3549
4.69.138.233   3356_3549 ae-2-52.ear1.NewYork2.Level3.net
4.69.138.233   3356_3549 ae-2-52.ear1.NewYork2.Level3.net
4.71.172.146   3356_3549 NEWSCORP.ear1.NewYork2.Level3.net
4.71.172.145   3356_3549 5-1-8-253.ear1.NewYork2.Level3.net    pt2pt
4.71.172.146   3356_3549 NEWSCORP.ear1.NewYork2.Level3.net

206.15.96.0/19
```

Customer-Provider Link   **Suggested Ingress ACL**

Goal: develop robust topological method to infer lack of ingress filtering

Customer or Provider Duty?

"Even if the customers are unaware of the spoofed traffic, ISPs should be aware which leaves them open for "aiding and abetting". This doesn't require inspecting the payload of the packets. This is the IP header which they are expected to examine and for which there is a BCP saying to drop spoofed packets. Sources are used for policy routing so the source field is expected to be processed.

I would expect a Judge to take into consideration the BCP in deciding whether a ISP should be aware of the issue when deciding if a ISP is aiding and abetting by allowing spoofed packets to enter their network."
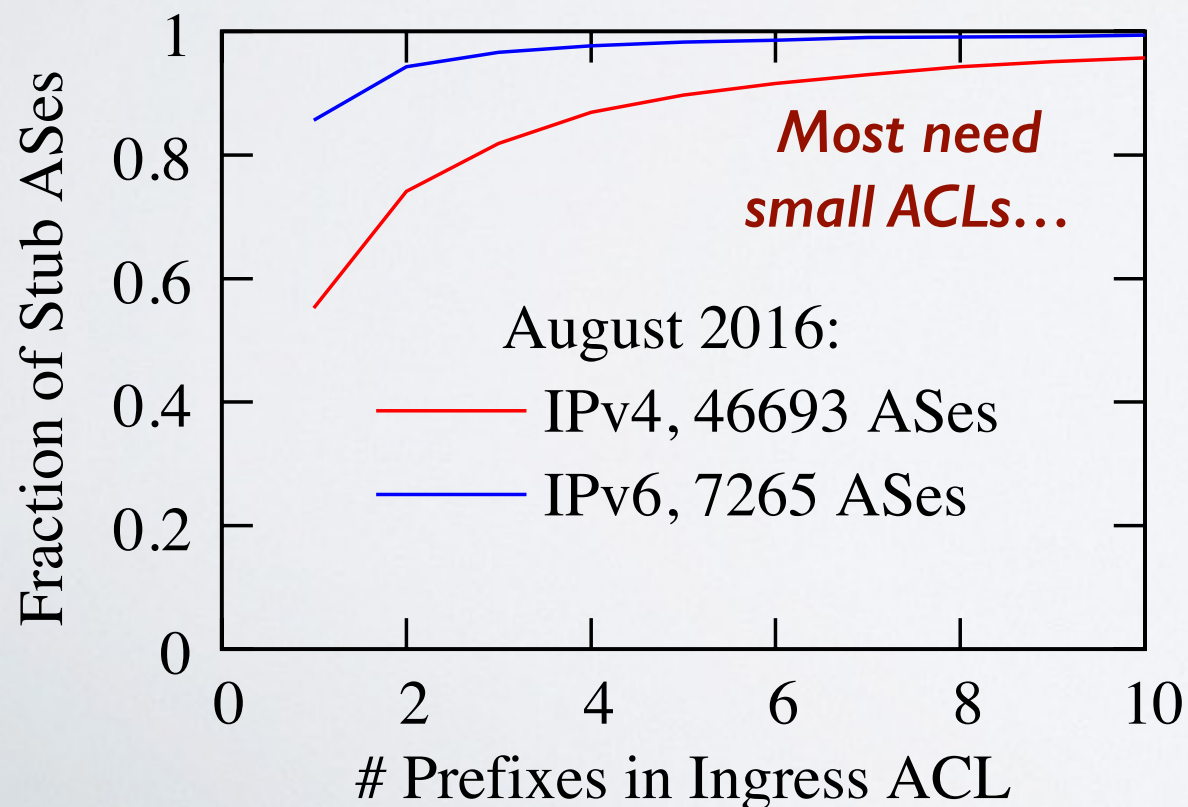
Mark @ ISC
http://mailman.nanog.org/pipermail/nanog/2016-September/088349.html

Time to Reconsider Defaults
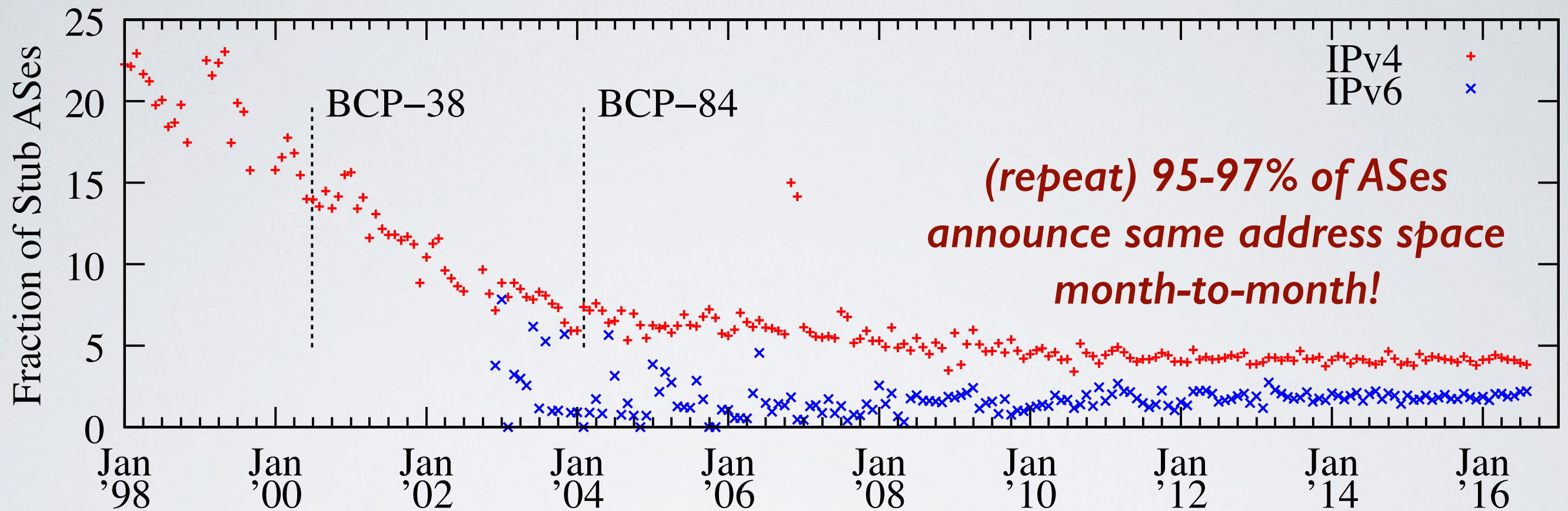
Where to from here?

- Would like to see the data have operational impact, improve health and hygiene of networks

  - This is where **you** come in! (https://spoofer.caida.org)

  - What problems do you encounter when trying to deploy filtering?

- Currently working on automated notification

  - emails to abuse contacts.

- Working on a per-provider view

  - which of my customer ASes can spoof?

Other sources of data

- Another view of spoofing is available via IXPs

  - traffic data (sanitized to only include MAC, src IP)

  - BGP customer cone data (e.g., from AS Rank)

  - list of ISP members at IXP

- Use this data to ascertain which interfaces are sending source addresses not in their customer cone

  - IXPs could use to notify members their BCP38 filter missing

  - Let us know if you are willing to help test software tool

Acknowledgments & References

- Project funded by U.S. Department of Homeland Security (DHS) Science and Technology (S&T) directorate

- NIST funded under same program to study performance impact of DDoS mitigation techniques
https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques

- Contact: spoofer-info@caida.org

- Download (please!): ***https://spoofer.caida.org***

- Donate (to any CAIDA Project):
http://www.caida.org/home/donate/