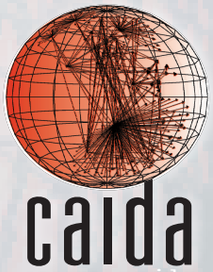
Software Systems for Surveying Spoofing Susceptibility

Matthew Luckie, Ken Keys, Ryan Koga,
Bradley Huffaker, Robert Beverly, kc claffy

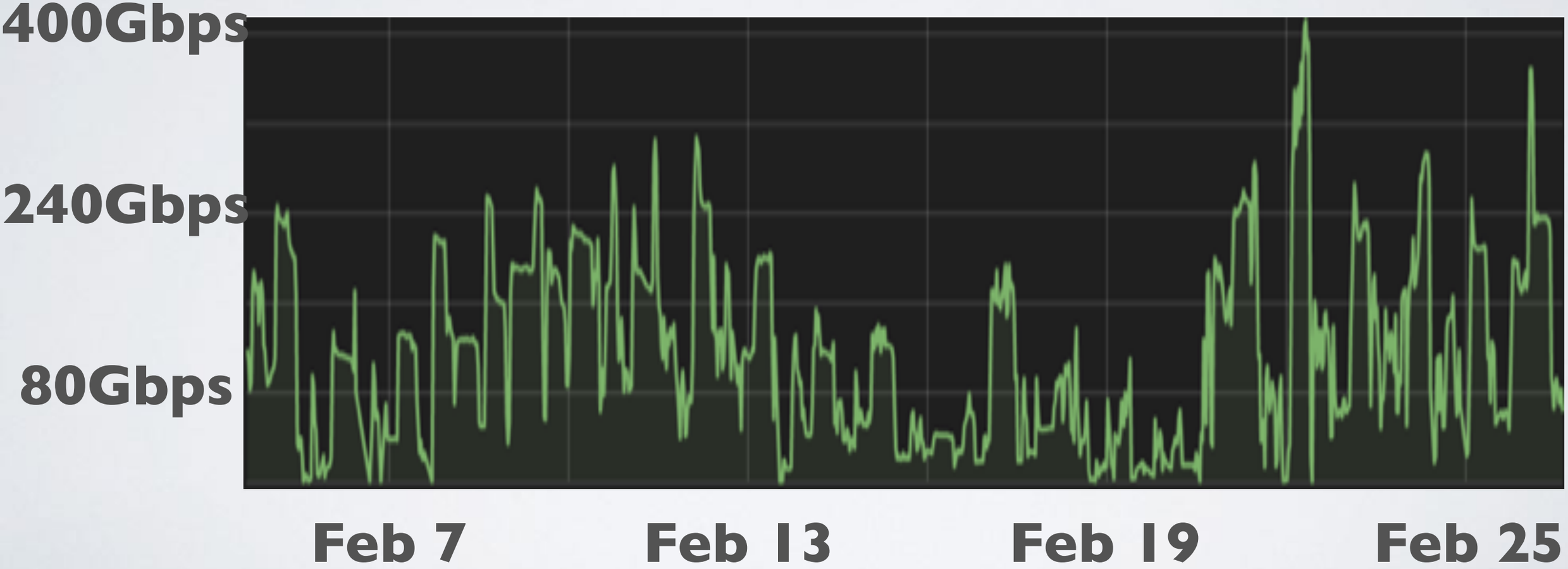
https://spoofer.caida.org/

NZNOG, January 26th 2017



What is the Problem?

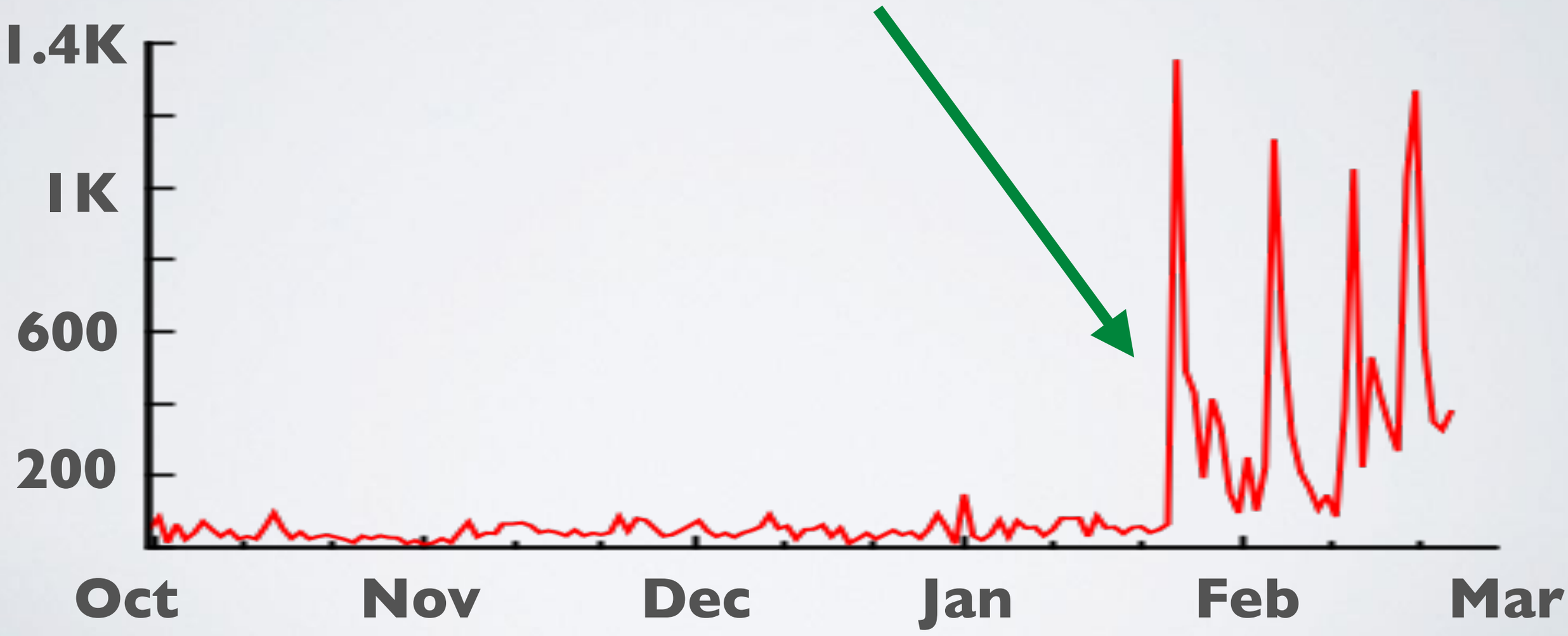
- Lack of filtering allows anonymous denial of service attacks.
- Example: CloudFlare reports **400Gbps attacks** on their systems through 2016



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

What is the Problem?

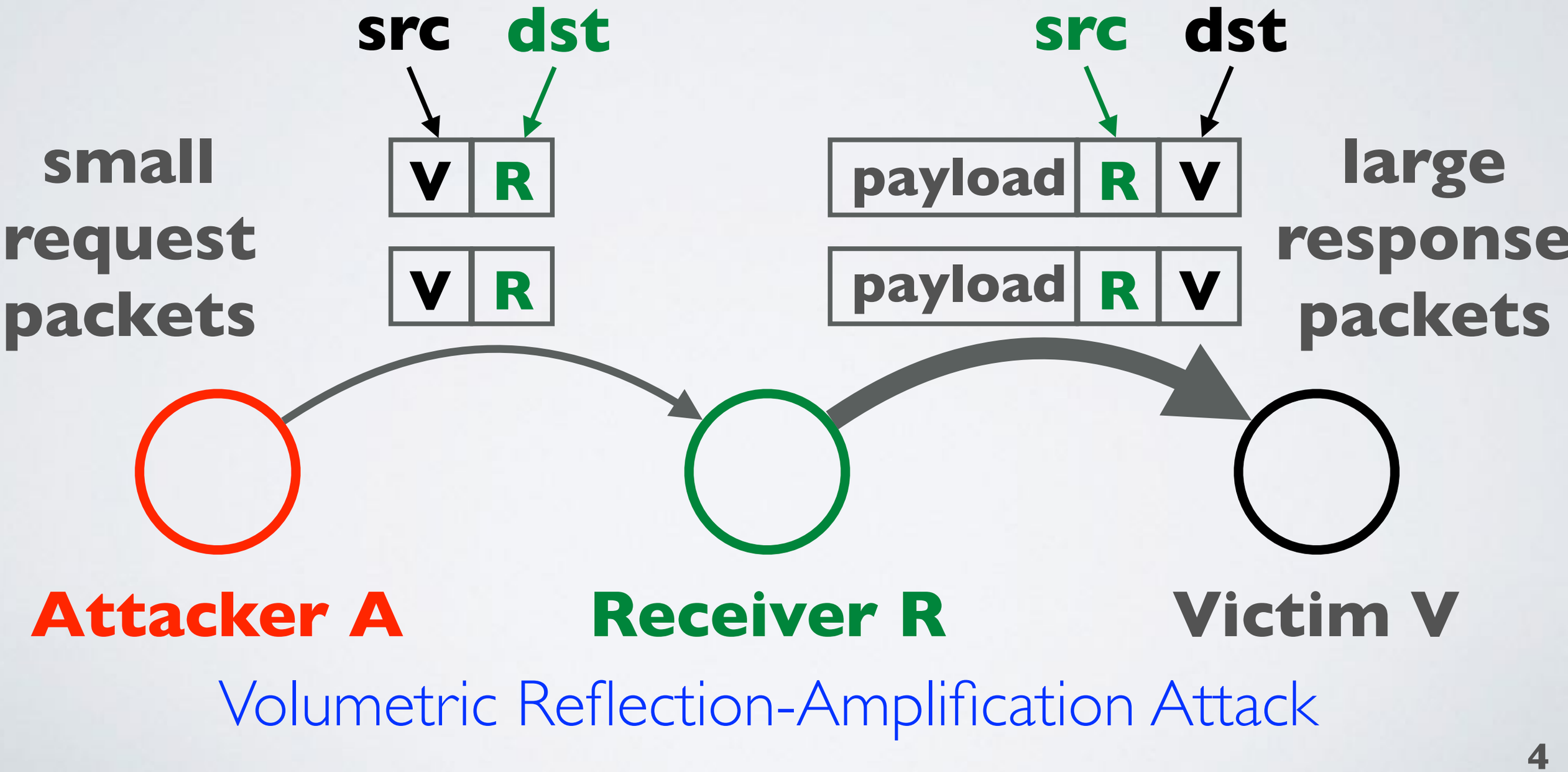
- Lack of filtering allows anonymous denial of service attacks.
- Example: CloudFlare reports **>1K DoS attack events** on their systems, per day, starting **Feb 2016**



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 always know if packet's source is authentic



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

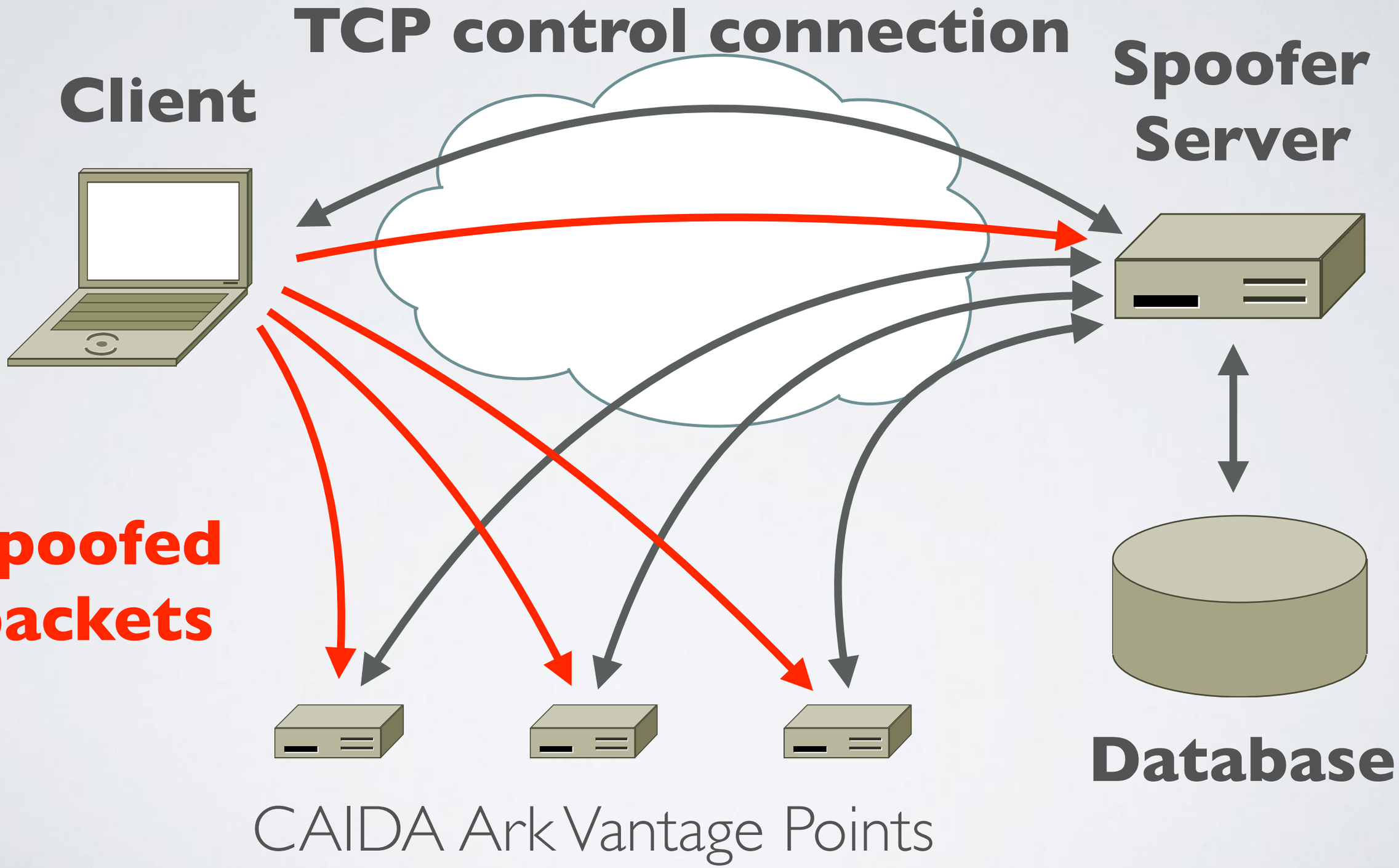
Tragedy of the Commons

- 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)

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**: aggregate statistics of spoofability based on crowd-sourced tests
  - user had to manually run tests

Spoofer: Client/Server Overview



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
  - opt-in to publicly share anonymized results, and opt-in to 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, and schedule tests
  - Speed improvements through parallelized probing

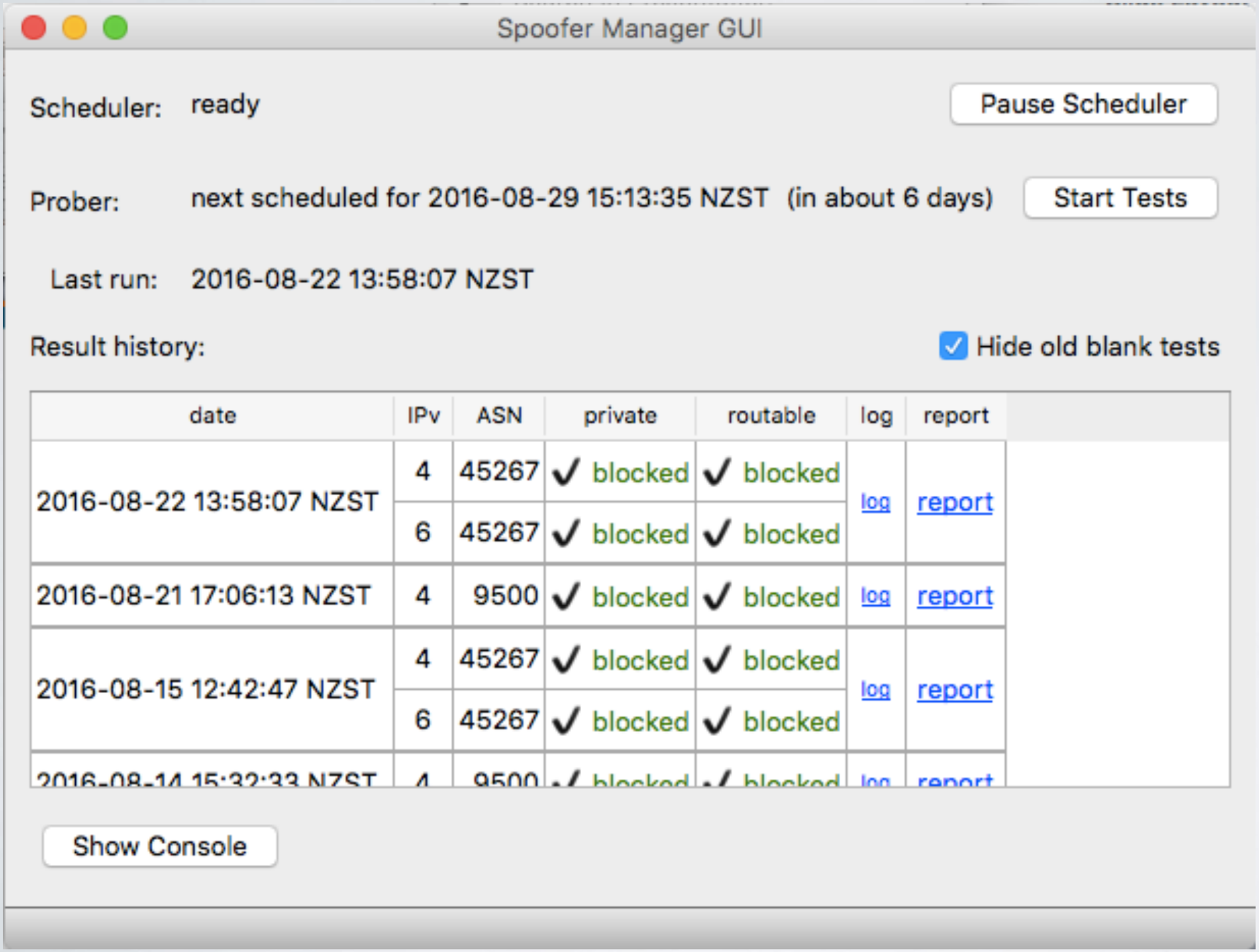
https://spoofer.caida.org/recent_tests.php

CAIDA Spoofer Project: New Features

- **Reporting Engine** publicly shows outcomes of sharable tests
  - Allows users to select outcomes
    - per country: which networks in a country need attention?
    - per ASN: which subnets need attention?
    - per provider: which of my BGP customers can spoof?
  - What address space does an AS announce, or could act as transit for? Is that address space stable?
    - Useful for deploying ACLs

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

Client GUI



Signed Installers

MacOS

Windows

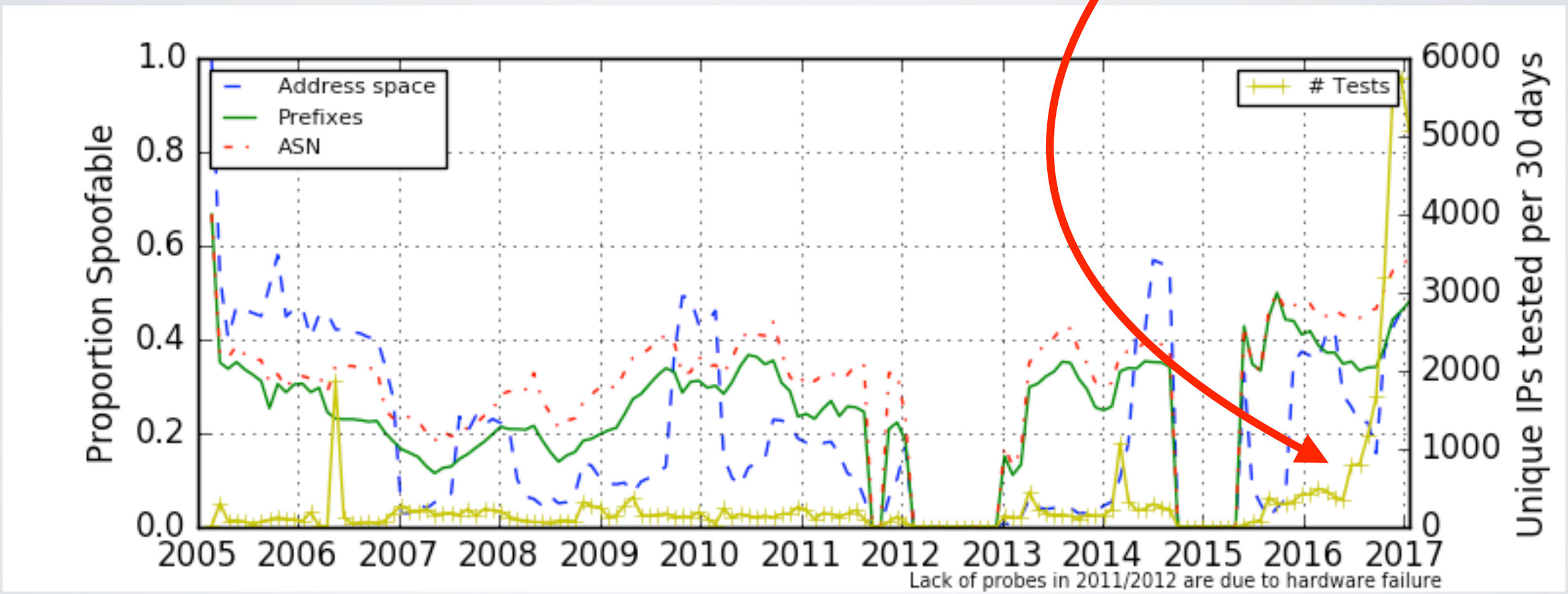
Linux

Open Source

C++

Client/Server Deployment

- Since releasing new client in May 2016, 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:cdxx::	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:b0xx::	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:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78405	2016-10-14 10:10:17	128.164.13.x	11039	usa					Full report
		2620:106:c0xx::	11039		no	blocked	blocked		
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:f3:80xx::	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								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:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78405	2016-10-14 10:10:17	128.164.13.x	11039	usa					Full report
		2620:106:c0xx::	11039		no	blocked	blocked		
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:f3:80xx::	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:cdxx::	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:b0xx::	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:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa					
78405	2016-10-14 10:10:17	128.164.13.x	11039	usa					
		2620:106:c0xx::	11039						
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:f3:80xx::	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	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

Addresses anonymized:
IPv4: /24
IPv6: /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:cdxx::	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:b0xx::	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:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55								Full report
78405	2016								Full report
78402	2016								Full report
78388	2016								Full report
78385	2016								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

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:cdxx::	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:b0xx::	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:c0xx::	11039		no	received	received		
78416	2016								Full report
78405	2016								Full report
78402	2016								Full report
78388	2016								Full report
78385	2016								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

Some spoofing from behind a NAT prevented by egress filtering

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:cdxx::	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:b0xx::	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:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
7840									Full report
7840									Full report
7838									Full report
7838									Full report
7838									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

Notifications and Remediation

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

Session	Timestamp	Client IP	ASN	Cou					
133390	2017-01-24 19:44:39	182.48.139.x	9245	nzl					
		2405:8400:10xx::	9245						
131277	2017-01-17 18:32:55	182.48.139.x	9245	nzl	no	blocked	blocked	/19	Full report
		2405:8400:10xx::	9245		no	blocked	blocked		
131065	2017-01-17 10:31:29	182.48.139.x	9245	nzl	no	blocked	blocked	/19	Full report
130402	2017-01-16 12:20:57	182.48.139.x	9245	nzl	no	blocked	blocked	/19	Full report
103356	2016-12-02 05:45:47	182.48.155.x	9245	nzl	yes	blocked	received	/8	Full report
103293	2016-12-02 04:02:44	182.48.155.x	9245	nzl	yes	blocked	received	/8	Full report
100969	2016-11-28 20:05:43	182.48.156.x	9245	nzl	yes	blocked	received	/8	Full report

Successful filtering deployment: weekly tests show spoofed packets are now blocked. Thanks, Compass.

Other Remediation Strategies

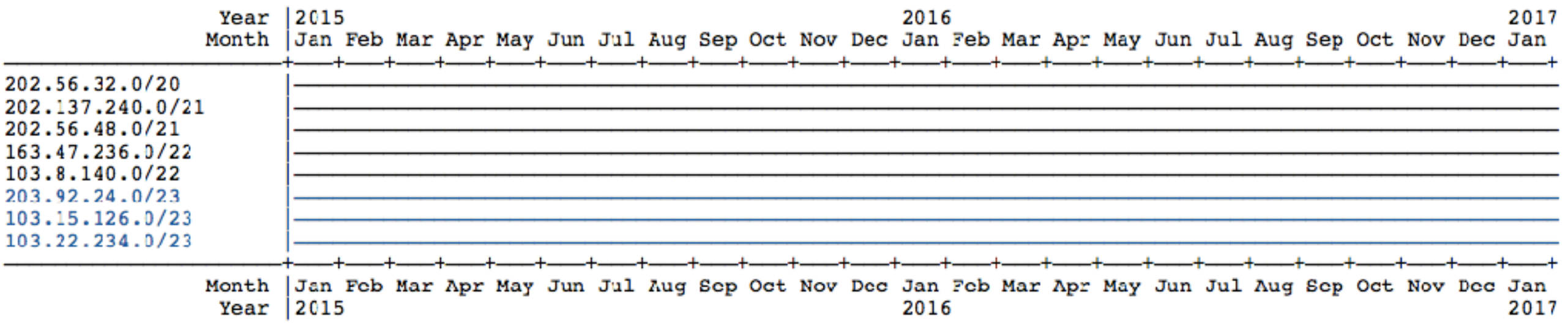
Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
126706	2017-01-10 17:01:46	202.137.245.x	9876	nzl	yes	received	received	/8	Full report
125897	2017-01-09 13:46:07	202.56.51.x	9876	nzl	yes	rewritten	rewritten	none	Full report
125800	2017-01-09 11:18:09	202.56.51.x	9876	nzl	yes	rewritten	rewritten	none	Full report
122417	2017-01-03 12:36:54	202.137.245.x	9876	nzl	yes	received	received	/8	Full report
115687	2016-12-21 12:22:00	202.137.245.x	9876	nzl	yes	received	received	/8	Full report
114563	2016-12-19 17:24:44	202.56.51.x	9876	nzl	yes	rewritten	rewritten	none	Full report
111334	2016-12-14 11:09:00	202.137.245.x	9876	nzl	yes	blocked	received	/8	Full report
110952	2016-12-14 00:17:50	202.56.51.x	9876	nzl	yes	rewritten	rewritten	none	Full report
106012	2016-12-06 15:17:56	202.137.245.x	9876	nzl	yes	blocked	received	/8	Full report
104151	2016-12-03 15:44:54	202.56.51.x	9876	nzl	yes	rewritten	rewritten	none	Full report
101573	2016-11-29 14:04:56	202.137.245.x	9876	nzl	yes	blocked	received	/8	Full report
97245	2016-11-22 12:51:56	202.137.245.x	9876	nzl	yes	blocked	received	/8	Full report
92300	2016-11-15 11:39:04	202.137.245.x	9876	nzl	yes	received	received	/8	Full report
88983	2016-11-10 16:57:29	202.56.51.x	9876	nzl	yes	rewritten	rewritten	none	Full report

AS9876, NOW Internet. Emailed abuse@ 26 Sept 2016.

Other Remediation Strategies

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

Address Space Announcements: 9876 (NOWNEW-AS-AP)



https://spoofer.caida.org/prefixes.php?asn=9876

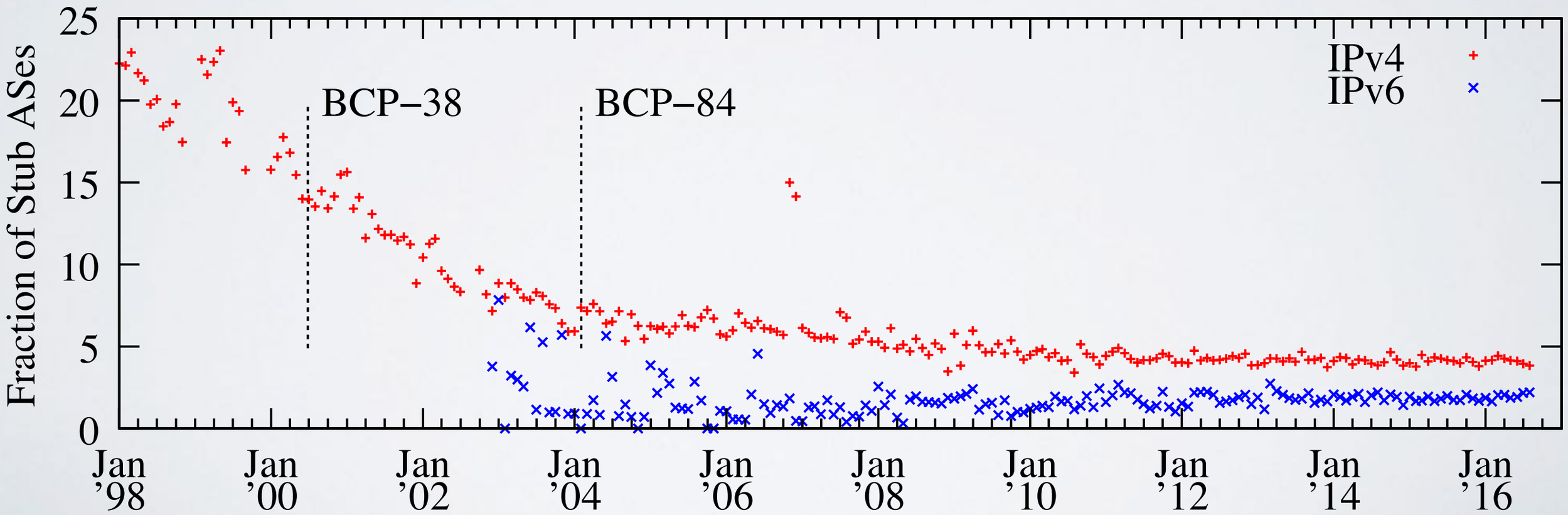
https://spoofer.caida.org/provider.php

Webpages by Stuart Thomson, Waikato

Practicality of 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.

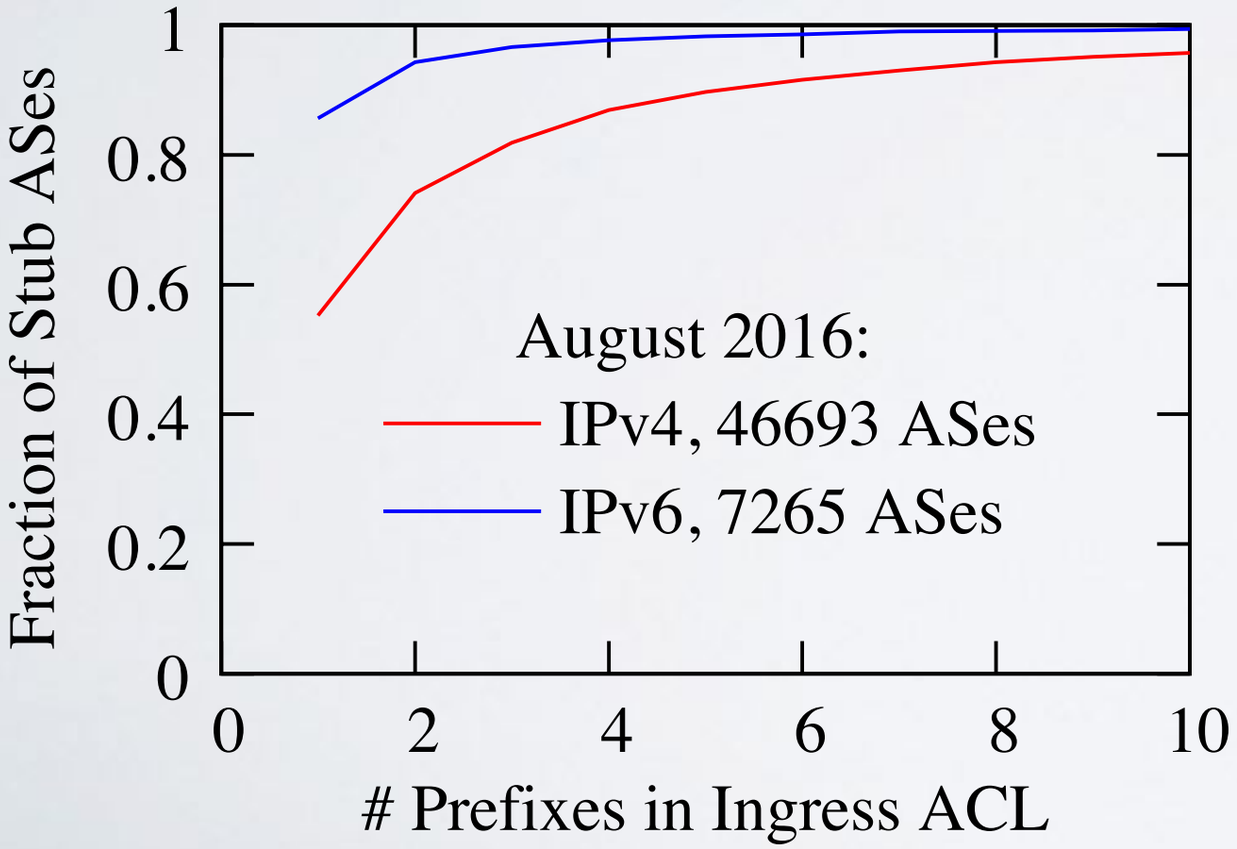


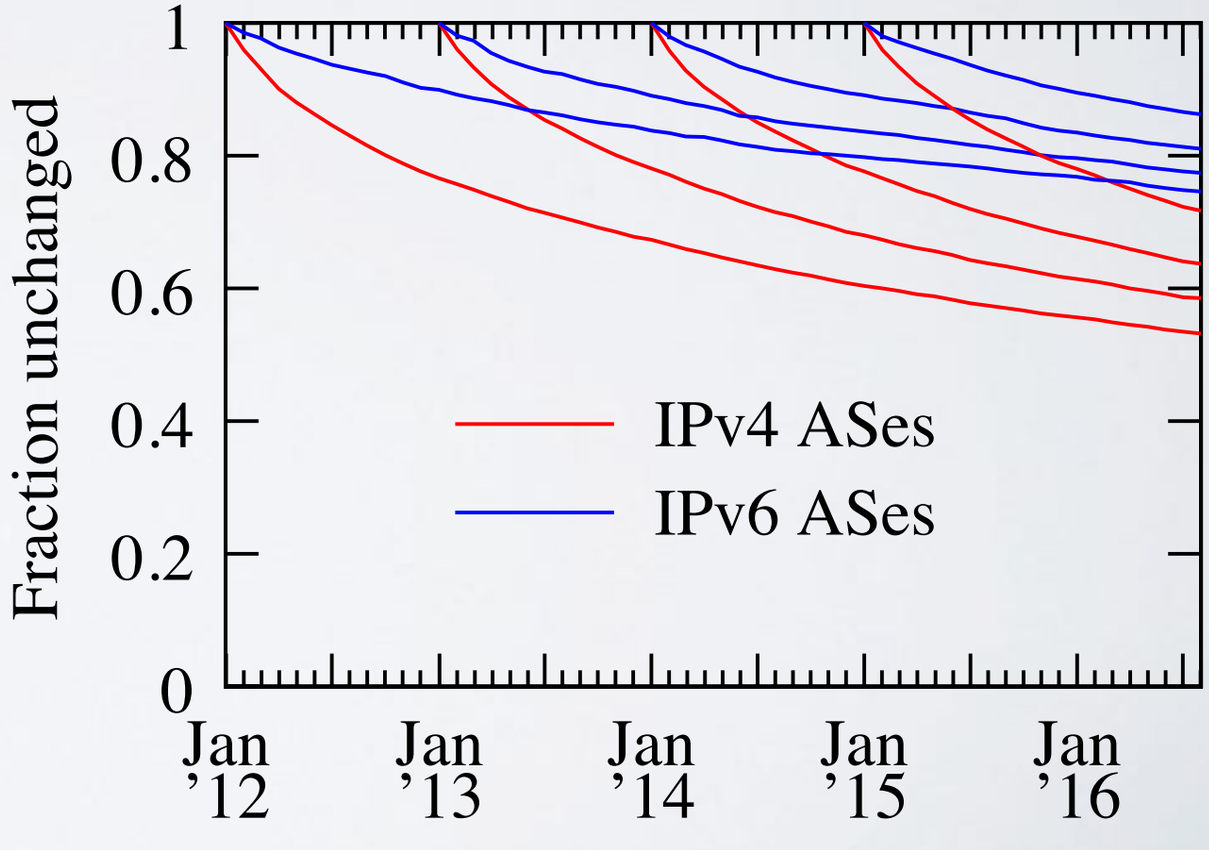
Source: Routeviews and RIPE RIS data

Practicality of 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.





Source: Routeviews and RIPE RIS data

Should I install the client?

- **Yes!**

- 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

Expanding View of Filtering Policy

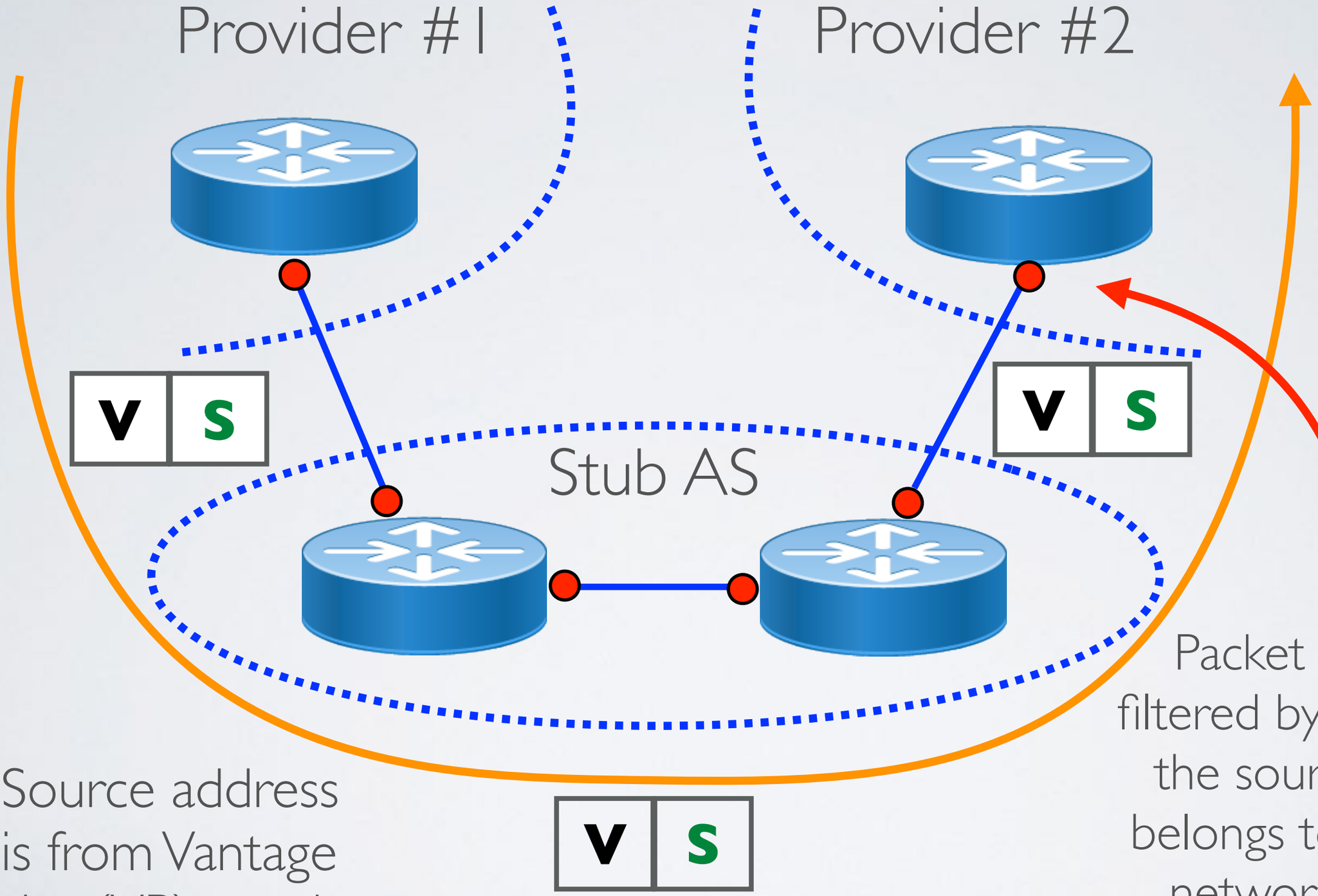
- Use CAIDA traceroute data to infer customer-provider links to stub ASes that imply lack of ingress filtering by provider

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

- Method suggested by Jared Mauch (NTT), joint work with Qasim Lone, Maciej Korczynski, Michel van Eeten (TU Delft)

https://spoofer.caida.org/trspoof.php

Traceroute Spoofer



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

https://spoofer.caida.org/trspoof.php

Summary

- **Reporting Engine** publicly shows outcomes of sharable tests, ~6K unique IPs in hundreds of ASNs per month.
  - Allows users to select outcomes
    - per country: which networks in a country need attention?
    - per ASN: which subnets need attention?
    - per provider: which of my BGP customers can spoof?
  - Allows operators to view address space announced by an AS announce, or could act as transit for, over time.
  - Please install and use the system!

https://spoofer.caida.org/

Acknowledgements

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

- Contacts:
  - spoofer-info@caida.org