Software Systems to Survey Spoofing Susceptibility

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

https://spoofer.caida.org/

SRI Arlington
11 April 2018

Homeland Security
Science and Technology

Team Profile

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

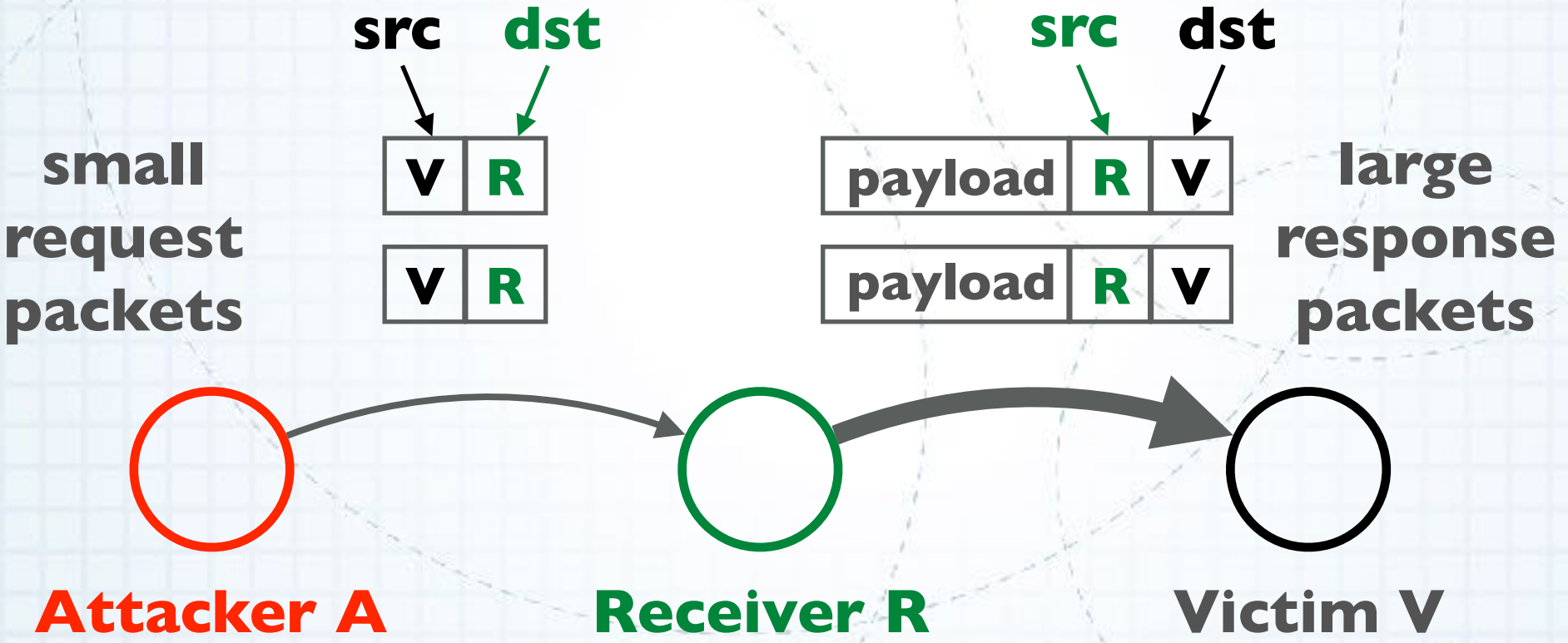
https://spoofer.caida.org/

Need: what is the problem?

- Lack of filtering allows anonymous denial of service attacks.
- Example: Akamai reported 1.3Tbps attack on their systems March 2018 (spoofed packets -> memcached amplification).
- Soon, thousands of attacks per day. Here we go again..
  - https://krebsonsecurity.com/2018/03/powerful-new-ddos-method-adds-extortion/
  - https://medium.com/@qratorlabs/the-memcached-amplification-attack-reaching-500-gbps-b439a7b83c98

Need: Why does spoofing matter?

- Attacker sends packet with spoofed source IP address
- Receiver cannot always know if packet's source IP is authentic



Volumetric Reflection-Amplification Attack

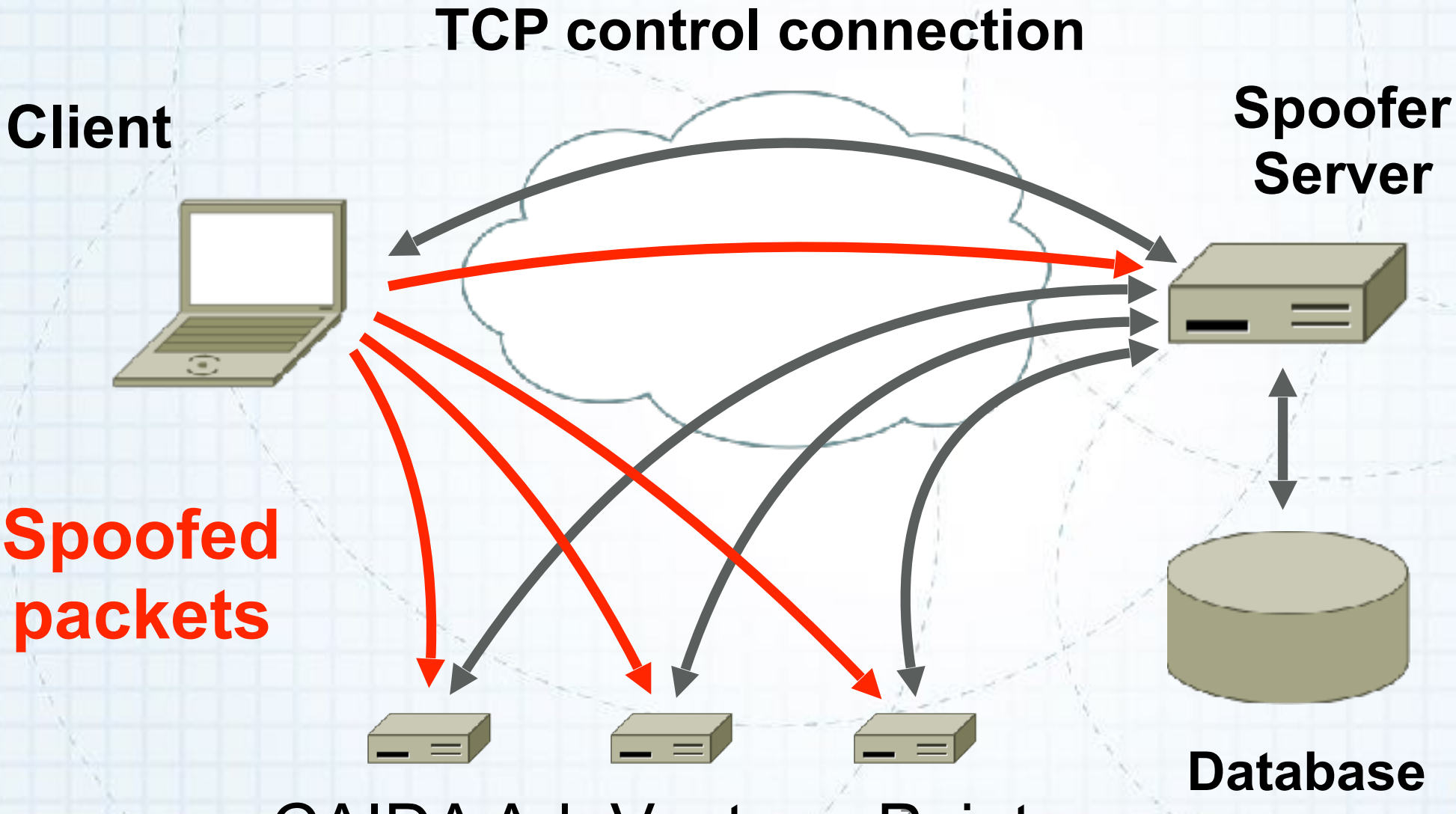
Existing “solutions” to spoofing

- **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 many networks.**
  - majority of networks do seem to deploy filtering. *But, no public data that allows a network to show that they have (or have not) deployed 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)

Spoofer: Client/Server Architecture



Spoofer: New Features

- **Client/Server** system provides new useful features
  - by default publish **anonymized** results, and
    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, and schedule tests
  - Speed improvements through parallelized probing

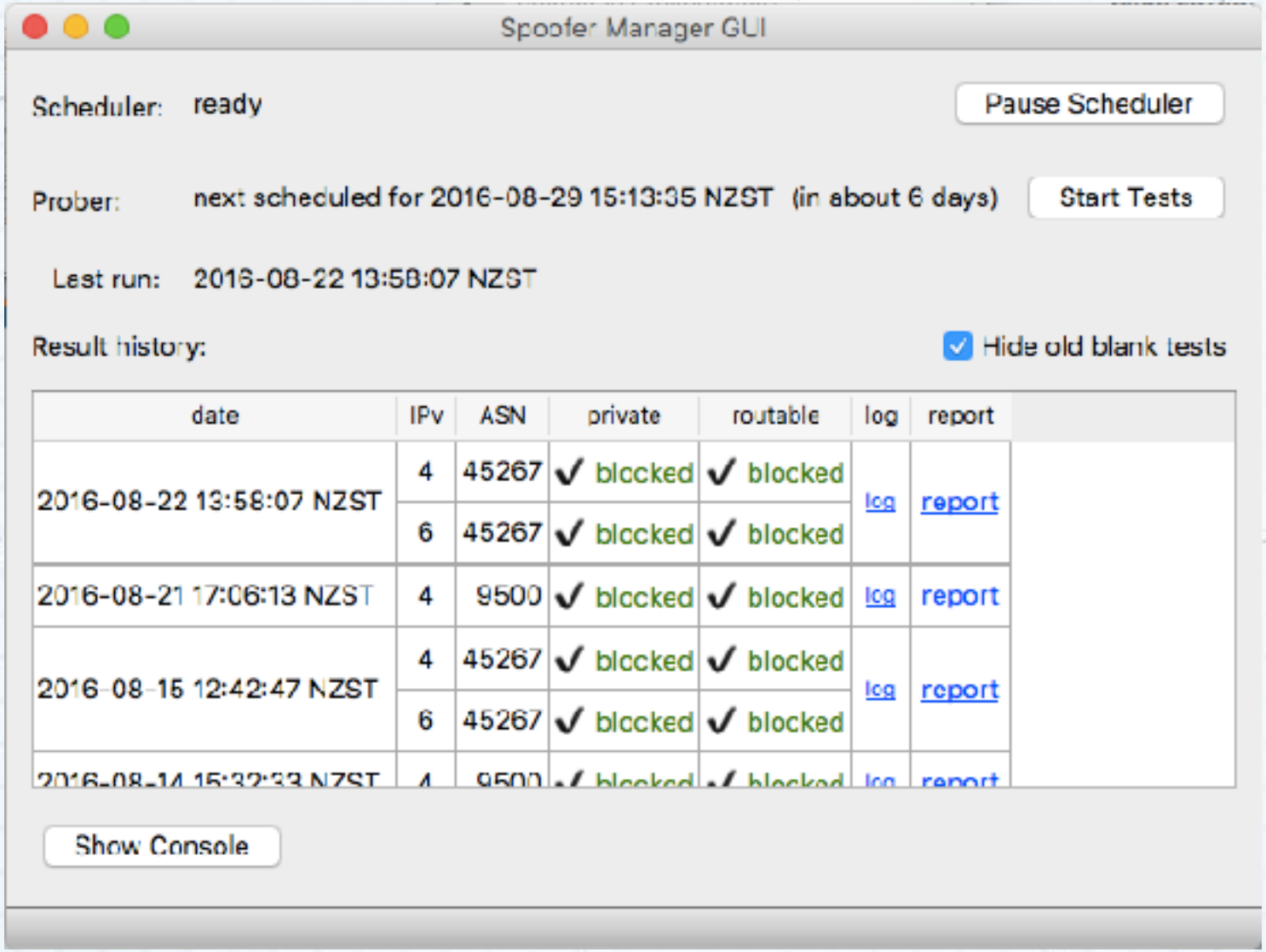
https://spoofer.caida.org/recent_tests.php

Spoofer: 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/as_stats.php

Spoofer Client GUI



Signed Installers

MacOS

Windows

Linux

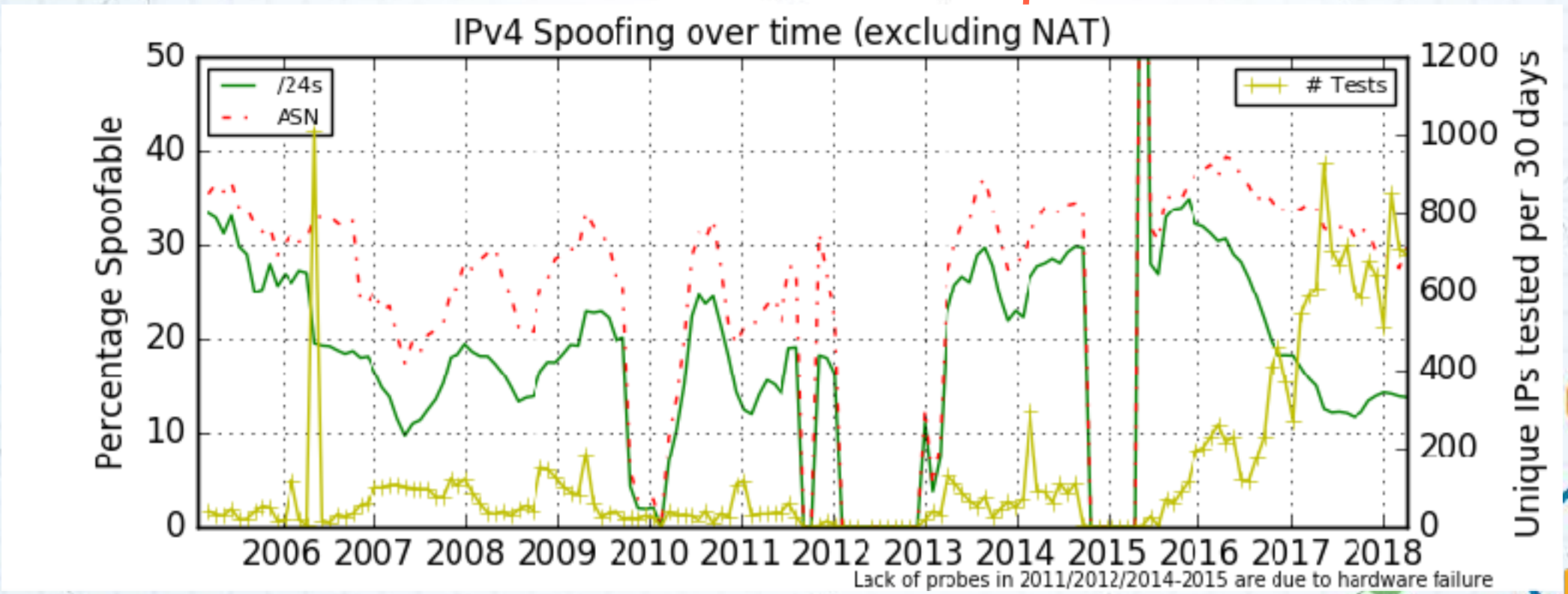
Open Source

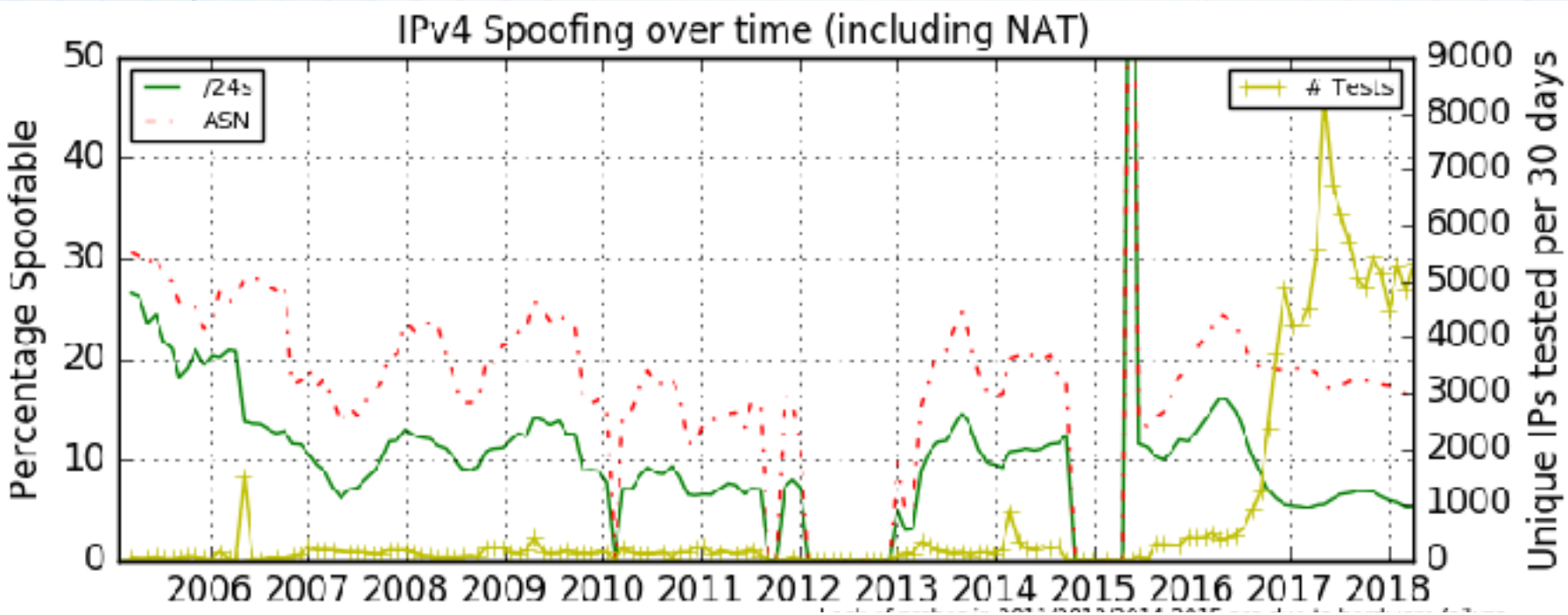
C++

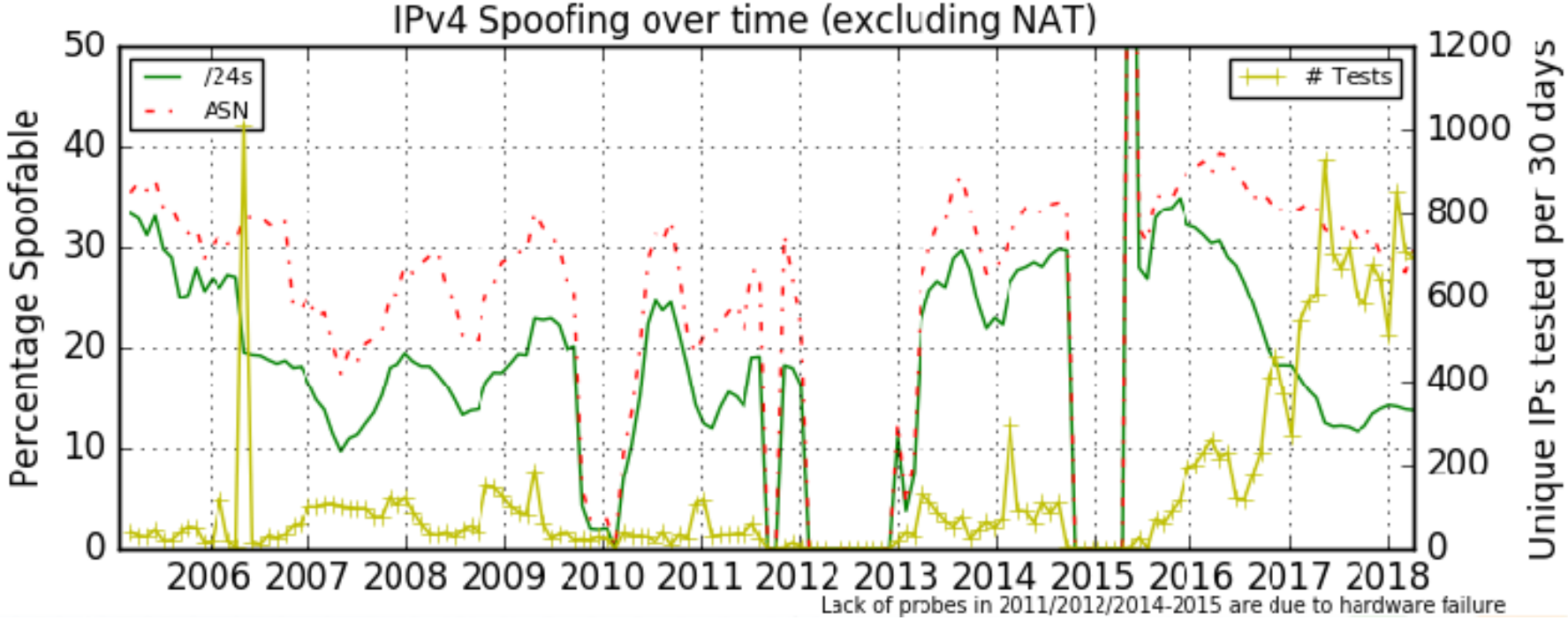
Client/Server Deployment

Since releasing new client in May 2016, huge jump in tests (yellow line)

Benefit of system running in background

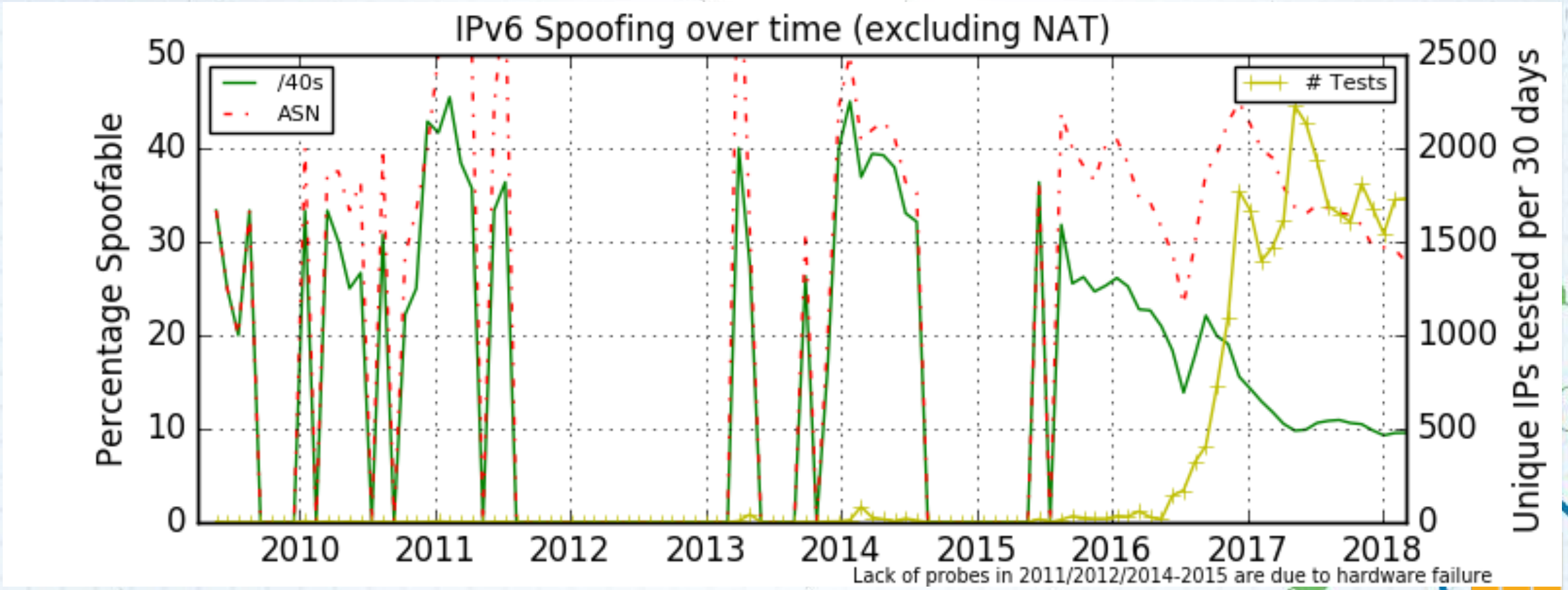






Excluding NATed IPs gives a likely more accurate inference for percentage of networks that allow spoofing. (Most NATs suppress spoofing.)

More unique IPv6 tests, lower rate of SAV 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	72.69.189.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								Full report
78405	2016-10								Full report
78402	2016-10								Full report
78388	2016-10								Full report
78385	2016-10								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
		2603:1007:b0xx::	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.69.189.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
		2620:105: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

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

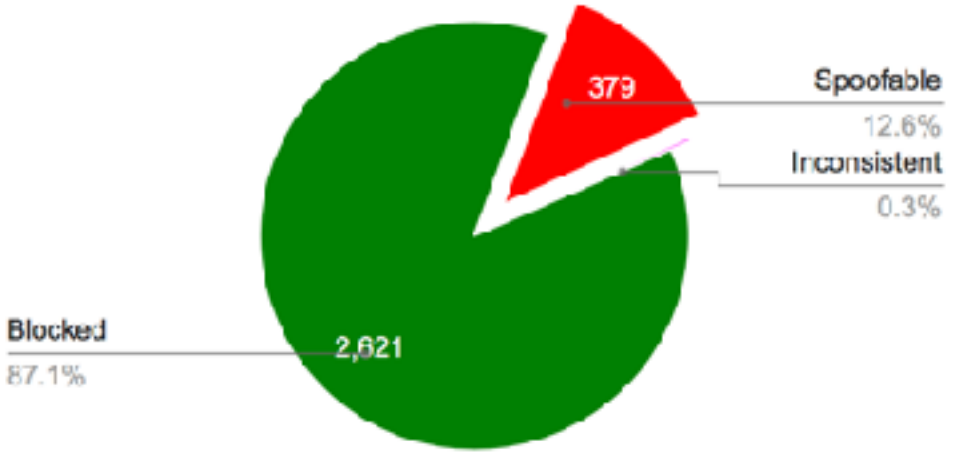
Reporting Engine: Recent Tests

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	72.69.189.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
		2620:105:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
784									Full report
784									Full report
783									Full report
783									Full report
783									Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

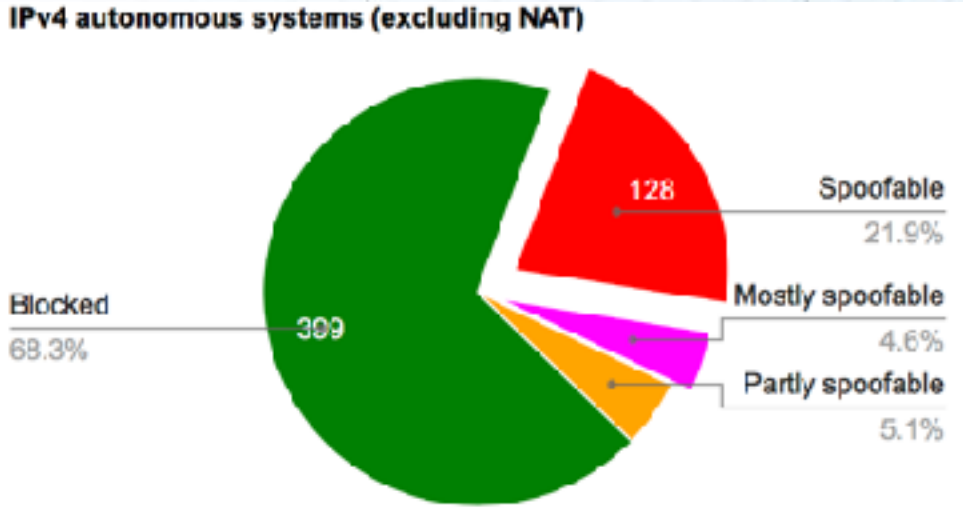
Some networks may have deployed IPv4 filtering, but forgotten to deploy IPv6 filtering

State of IP Spoofing (last 12 mo)

IPv4 Blocks (Excluding NAT)



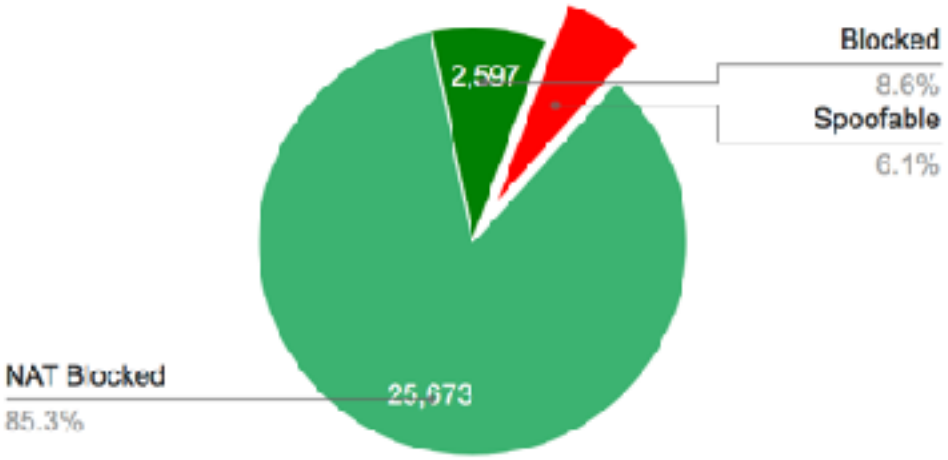
Status	Count
Spoofable	379
Inconsistent	8
Blocked	2621



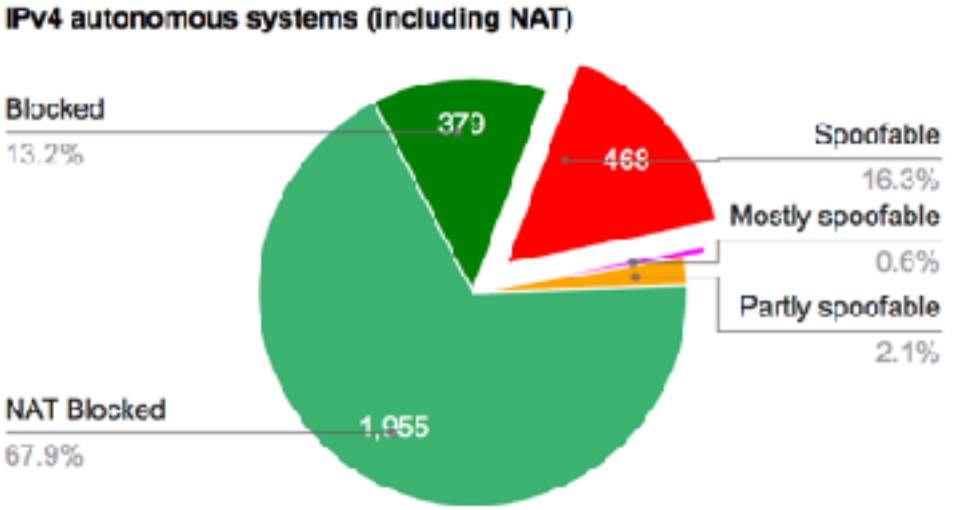
Status	Count
Spoofable	128
Mostly spoofable	27
Partly spoofable	30
Blocked	399

State of IP Spoofing (last 12 mo)

IPv4 Blocks (Including NAT)



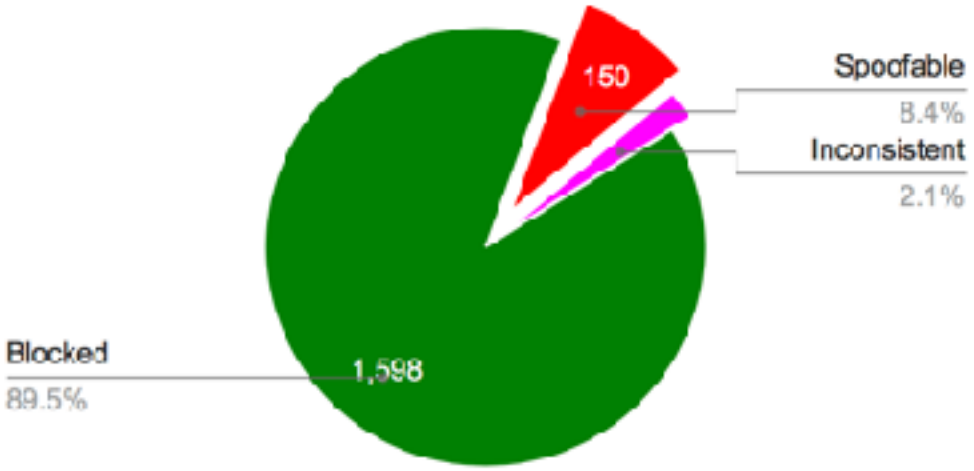
Status	Count
Spoofable	1826
Inconsistent	7
NAT Blocked	25673
Blocked	2597



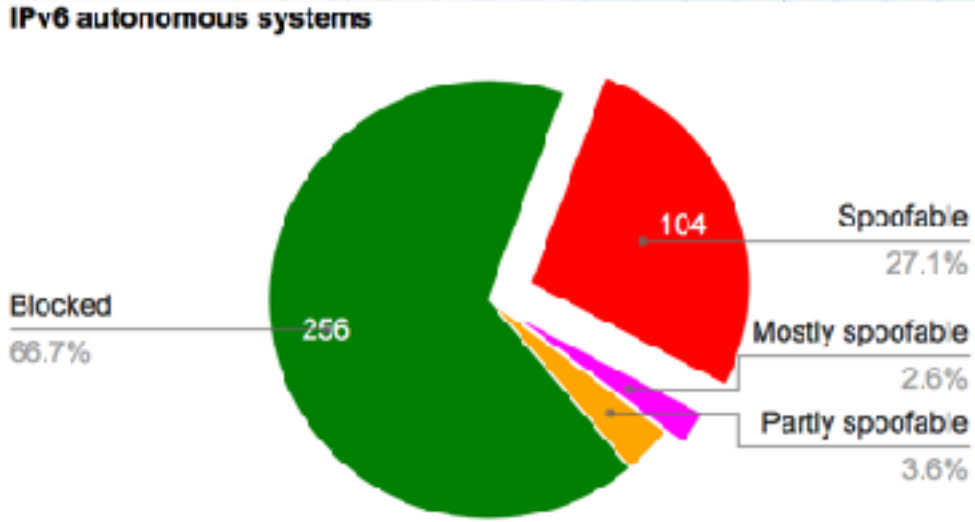
Status	Count
Spoofable	468
Mostly spoofable	16
Partly spoofable	61
NAT Blocked	1955
Blocked	379

State of IP Spoofing

IPv6 Blocks and Autonomous Systems



Status	Count
Spoofable	150
Inconsistent	38
Blocked	1598



Status	Count
Spoofable	104
Mostly spoofable	10
Partly spoofable	14
Blocked	256

Notifications and Remediation

- Currently, we (Matthew) send (semi-automated) notifications to abuse contacts of prefixes from which we received a spoofed packet.

Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 /… S…	
133390	2017-01-24 19:44:39	182.48.139.x	9245	nzl	no	blocked	blocked	/19	
		2405:8400:10xx::	9245		no	blocked	blocked		
131277	2017-01-17 18:32:55	182.48.139.x	9245	nzl	no	blocked	blocked	/19	
		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.

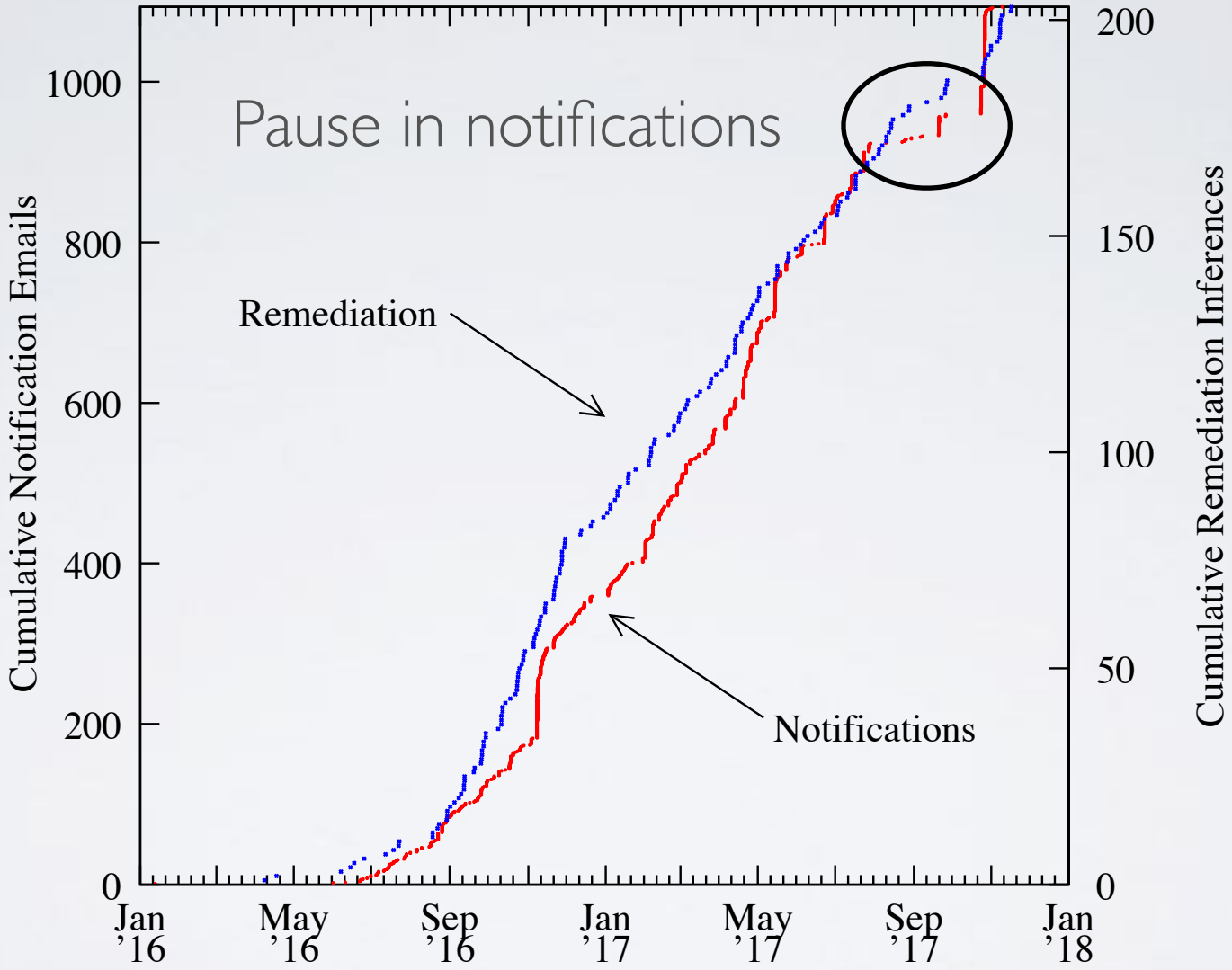
- remediation rate: 1/5 ASes in majority native English-speaking
- 1/6 for rest

Growing evidence of remediation

ASN	Country	IP Address	Received Timestamp	Blocked Timestamp
9299 (IPG-AS-AP)	phl (Philippines)	122.52.49.x/24	2017-05-15 19:25:17	2017-05-16 15:30:12
11039 (GWU)	usa (United States)	2620:108:c0xx::/40	2017-05-16 08:36:16	2017-05-16 11:47:20
209 (CENTURYLINK-US-LEGACY-QWEST)	usa (United States)	75.4.117.x/24	2017-05-11 19:40:23	2017-05-15 19:32:58
135301	aus (Australia)	103.90.236.x/24	2017-05-14 23:45:56	2017-05-14 23:53:08
2121 (RIPE MEETING AS)	dnk (Denmark)	2001:67c:xx::/40	2017-05-08 00:35:44	2017-05-09 01:13:52
209 (CENTURYLINK-US-LEGACY-QWEST)	usa (United States)	75.4.126.x/24	2017-05-08 11:17:23	2017-05-08 19:20:16
1653 (SUNET)	swe (Sweden)	193.10.0.x/24	2016-12-16 06:12:06	2017-05-02 08:49:54
1653 (SUNET)	swe (Sweden)	2001:6b0:xx::/40	2017-05-02 01:36:01	2017-05-02 08:00:56
7018 (ATT-INTERNET4)	usa (United States)	172.9.21.x/24	2017-03-16 21:27:30	2017-04-30 19:16:59
38152 (KCEC ASN)	usa (United States)	2607:f768:2xx::/40	2017-04-27 09:35:22	2017-04-27 11:46:24
39980 (PAF)	swe (Sweden)	192.165.72.x/24	2017-04-07 12:11:32	2017-04-26 11:04:00
197922 (FIRSTHEBERG)	fra (France)	93.113.200.x/24	2017-04-21 01:56:10	2017-04-23 11:10:15
31857 (PRIORITY TERABIT)	usa (United States)	69.28.82.x/24	2017-04-12 03:27:36	2017-04-19 04:41:54
237 (MERIT-AS-14)	usa (United States)	2001:48a8:68xx::/40	2017-03-08 13:46:43	2017-04-18 09:40:02
237 (MERIT-AS-14)	usa (United States)	198.108.63.x/24	2017-02-20 10:39:26	2017-04-18 09:40:02
21804 (ACCESS-SK)	can (Canada)	24.72.6.x/24	2017-02-20 15:08:53	2017-04-14 08:41:04
39980 (PAF)	swe (Sweden)	192.165.72.x/24	2017-04-11 02:24:34	2017-04-13 06:09:25
34244 (TELESERVICE)	swe (Sweden)	2a02:80:3fxx::/40	2017-04-11 02:24:34	2017-04-13 06:09:25
24217 (DETIK-AS-ID)	idn (Indonesia)	103.49.221.x/24	2017-04-11 00:31:13	2017-04-12 20:16:47
32107 (WAVE-CABLE)	usa (United States)	24.113.209.x/24	2017-04-07 18:23:10	2017-04-07 20:41:16
237 (MERIT-AS-14)	usa (United States)	198.108.53.x/24	2017-03-08 13:46:43	2017-04-06 11:12:19
13857 (ONLINEMAC)	usa (United States)	206.212.236.x/24	2016-11-03 09:21:30	2017-04-05 13:12:24
4608 (APNIC-SERVICES)	nld (Netherlands)	2001:dd0:a0xx::/40	2016-11-20 20:27:08	2017-04-02 18:36:45
7922 (COMCAST-7922)	usa (United States)	2601:601:80xx::/40	2017-03-21 22:00:13	2017-03-29 09:26:05
394437 (PSLIGHTWAVE)	usa (United States)	2606:a780:xx::/42	2016-11-03 17:31:21	2017-03-25 09:44:26
7018 (ATT-INTERNET4)	usa (United States)	99.92.143.x/24	2017-03-17 23:01:37	2017-03-24 22:34:09
237 (MERIT-AS-14)	usa (United States)	198.108.60.x/24	2017-03-10 18:43:20	2017-03-23 15:18:54

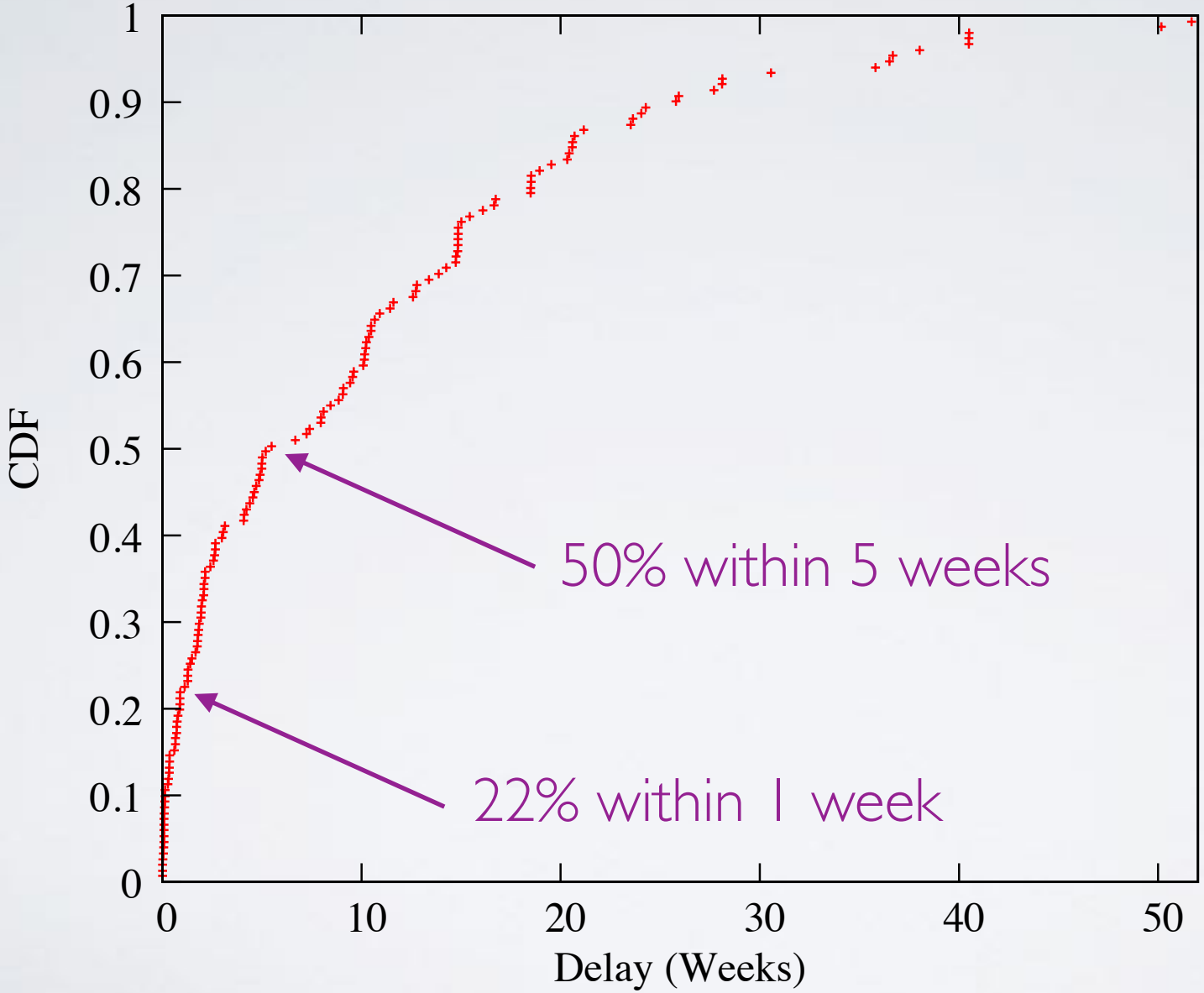
https://spoofer.caida.org/remedy.php

Notifications and Remediation



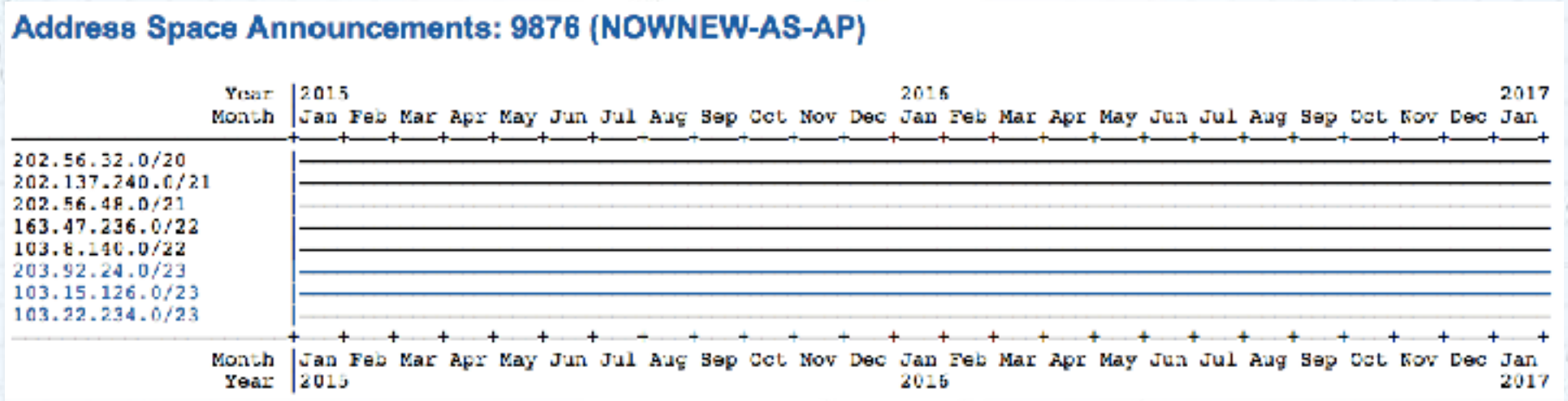
Sent 1061 private notifications, 203 remediation inferences

Delay from Notification to Remediation



Other Remediation Strategies

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



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

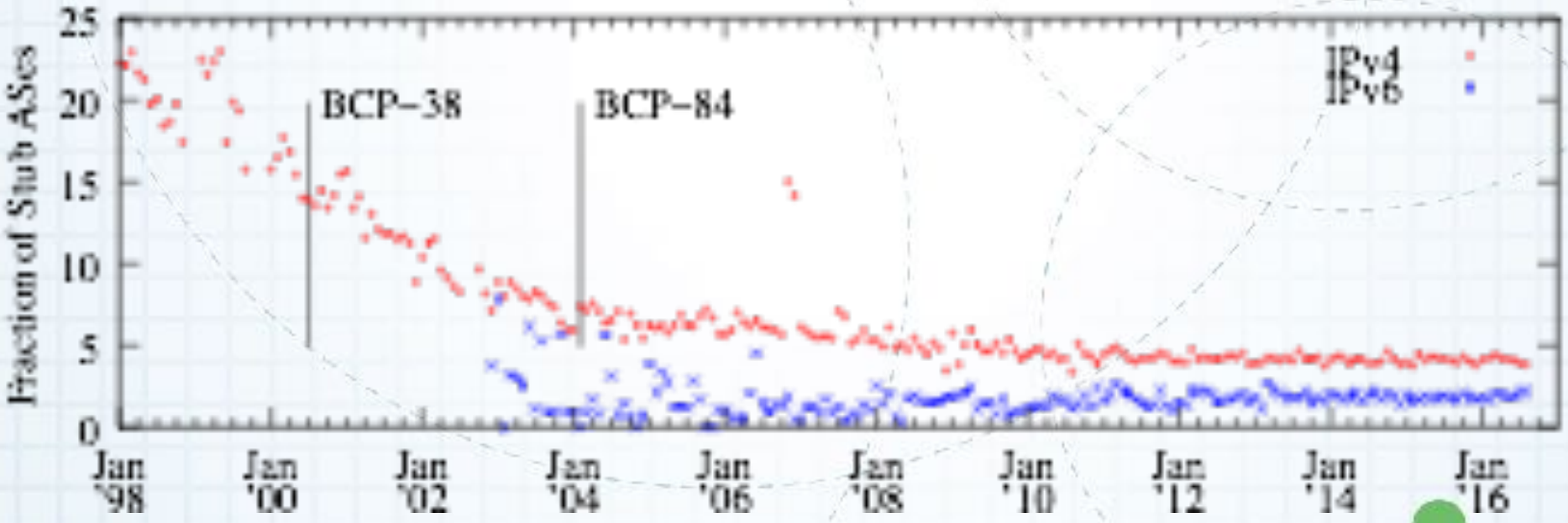
https://spoofer.caida.org/provider.php

[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.

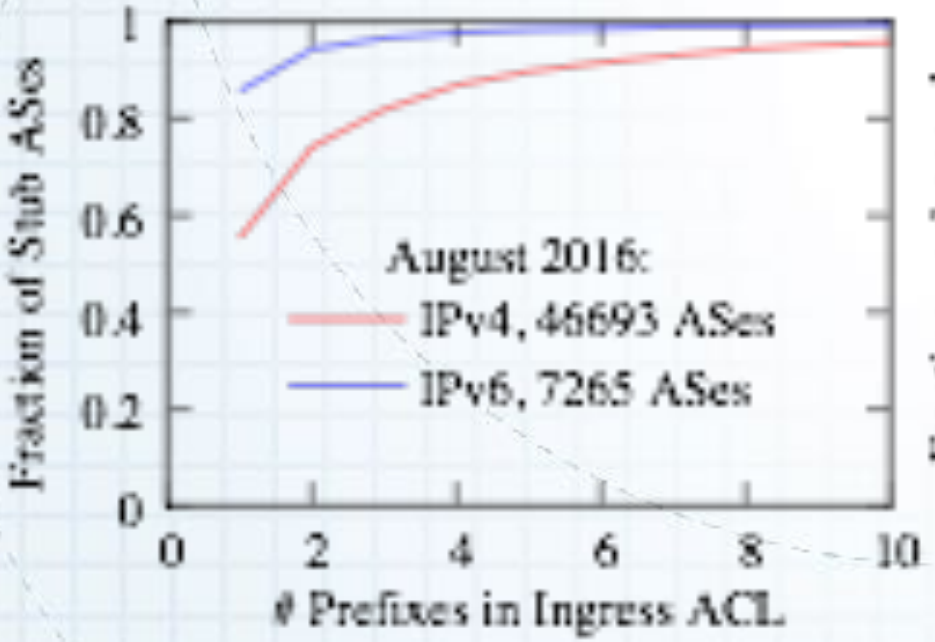


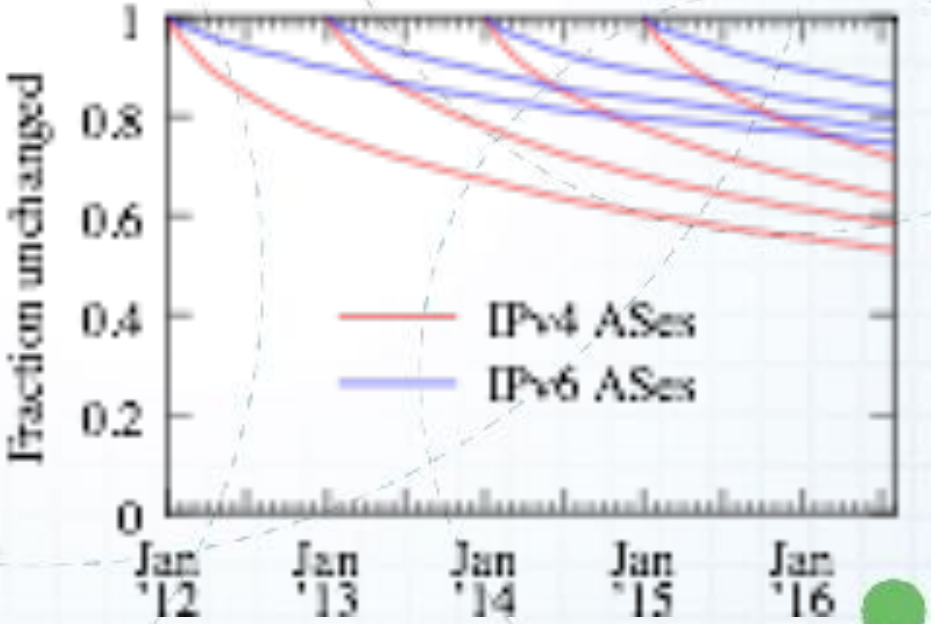
Data Source: Routeviews and RIPE RIS data

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 be the same today.





Data Source: Routeviews and RIPE RIS data

Other Remediation Strategies

- **Enhanced data access to authorities**
  - All tests in given country, network (unanonymized)
- **Language translation of notifications**
  - Not in current DHS contract
  - ICANN helping with translation of notification language
- **Region-specific emails to operator mailing lists**
  - Have presented to NANOG, NZNOG, AusNOG meetings
  - Private notifications to all observably spoofing networks
  - Latest: region-specific network operator group focus

Region-specific operator focus

In response to feedback from operational security communities,
CAIDA's source address validation measurement project
(https://spoofer.caida.org) is automatically generating monthly
reports of ASes originating prefixes in BGP for systems from which
we received packets with a spoofed source address.
We are publishing these reports to network and security operations
lists in order to ensure this information reaches operational
contacts in these ASes.

This report summarises tests conducted within usa, can.

Inferred improvements during Mar 2018:

ASN	Name	First-Fixed
11232	MIDCO-NET	2018-03-28
40801	LEWISU-ROMEOVILLE	2018-03-28
33651	CMCS	2018-03-29
7018	ATT-INTERNET4	2018-03-31

Further information for the inferred remediation is available at:
https://spoofer.caida.org/remedy.php

Source Address Validation issues inferred during Mar 2018:

ASN	Name	First-Spoofed	Last-Spoofed
577	BACOM	2016-03-09	2018-03-31
7029	WINDSTREAM	2016-06-21	2018-03-20
209	CENTURYLINK-US-LEGACY-QWEST	2016-08-16	2018-03-25
11232	MIDCO-NET	2016-09-22	2018-03-24
20412	CLARITY-TELECOM	2016-09-30	2018-03-31
6181	FUSE-NET	2016-10-10	2018-03-25
62482	AS-LRCOMM	2016-10-21	2018-03-07
15305	SYRINGANETWORKS	2016-10-21	2018-03-28
25787	ROWE-NETWORKS	2016-10-21	2018-03-30
174	COGENT-174	2016-10-21	2018-03-28
271	BCNET-AS	2016-10-24	2018-03-23
32440	LONI	2016-11-03	2018-03-29
33182	DIMENOC	2016-11-08	2018-03-28
12083	WOW-INTERNET	2016-11-09	2018-03-29
5056	AUREON-5056	2016-11-10	2018-03-30

First auto-generated email to NANOG this week

Will send region-specific recent-test data to operational mailing lists, every month

Current Status

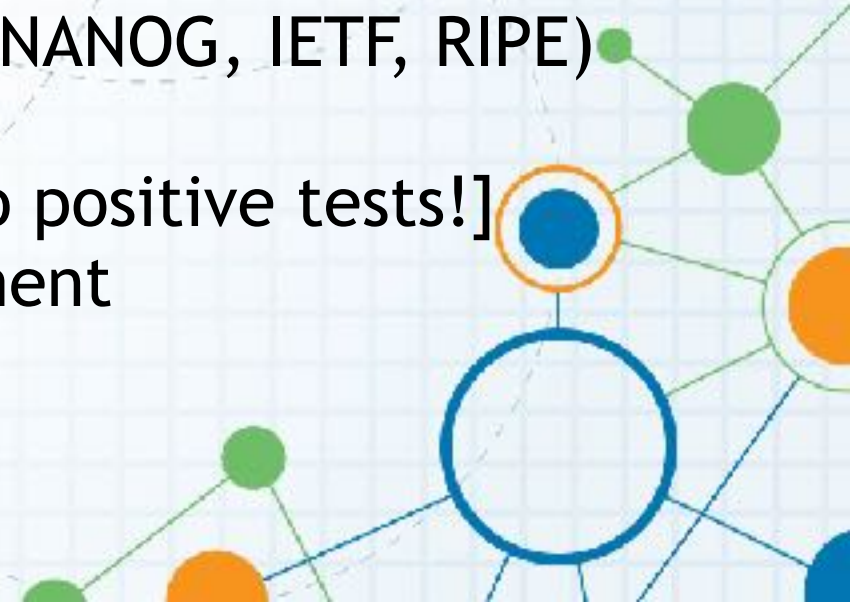
- Period I: Applied Research and Development (8 months, August 1, 2015 - March 31, 2016) - completed
- Period II: Development (12 months, April 1, 2016 - March 31, 2017) - completed
- Period III: Development and Technology Demonstration (16 months, April 1, 2017 - July 31, 2018)
  - Task 1: Refine client-server SAV testing technology and reports according to experiences and feedback, with continuing releases as necessary
  - Task 2: Develop software client for deployment in resource-constrained open-source home routers

Milestones and Deliverables (Period III)

- **Updated reporting system includes information about clients receiving spoofed packets**
- **Released software tool to measure ISP SAV deployment and identify a lack of ingress filtering by providers**

Lessons Learned

1) Remediation is a hard problem to solve
   - Rarely do we get to interact with someone to whom we send a notification
2) Tests are still more sparse than we expected
   - Not common to have multiple tests from same prefix
3) Lack of peer pressure (or other incentives) contributes to problem
   - We gave talks at NANOG, NZNOG, etc.
   - Even networks stood up by operator groups (NANOG, IETF, RIPE) often do not have SAV configured properly
     [Kudos for RIPE's Oct. meeting network, no positive tests!]
4) Any step forward requires this sort of measurement



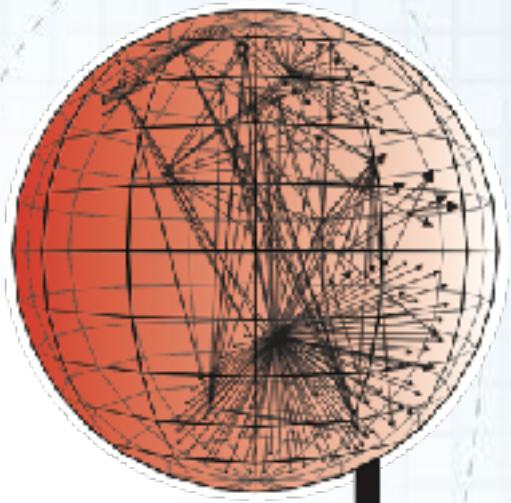
Should I install the client?

- **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

https://spoofer.caida.org/

spoofer-info@caida.org

k claffy
CAIDA/UCSD
kc@caida.org
858-534-8333
twitter:@caidaorg



caida

SDSC
SAN DIEGO SUPERCOMPUTER CENTER

UC San Diego

THANK YOU!

(Software Systems to Survey Spoofing Susceptibility)

(kc | UCSD | spoofer-info@caida.org)

This technology has been funded by DHS S&T Cyber Security Division.
For more information, contact SandT-Cyber-Liaison@hq.dhs.gov

Homeland Security

Science and Technology