Software Systems for Surveying Spoofing Susceptibility

k claffy / CAIDA/UCSD

July 26-27, 2017

Homeland Security

Science and Technology

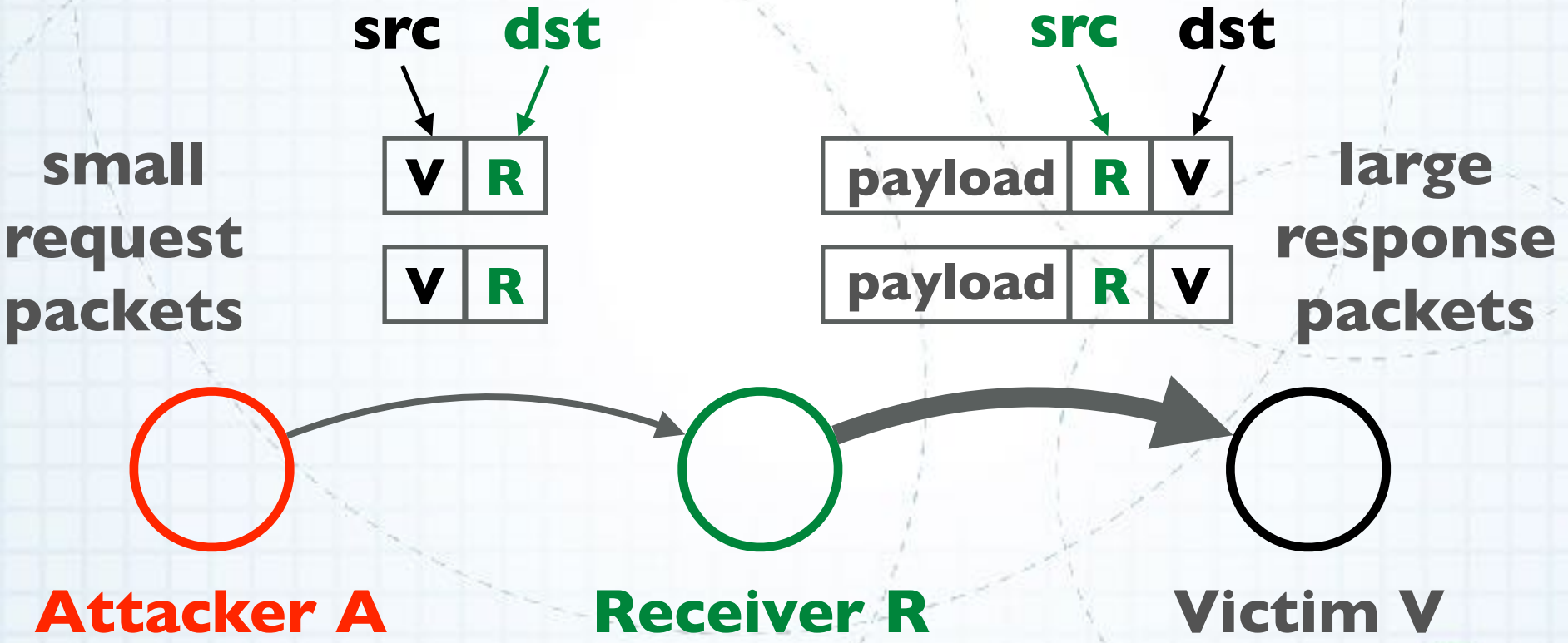
Team Profile

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

https://spoofer.caida.org/

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”

- **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.

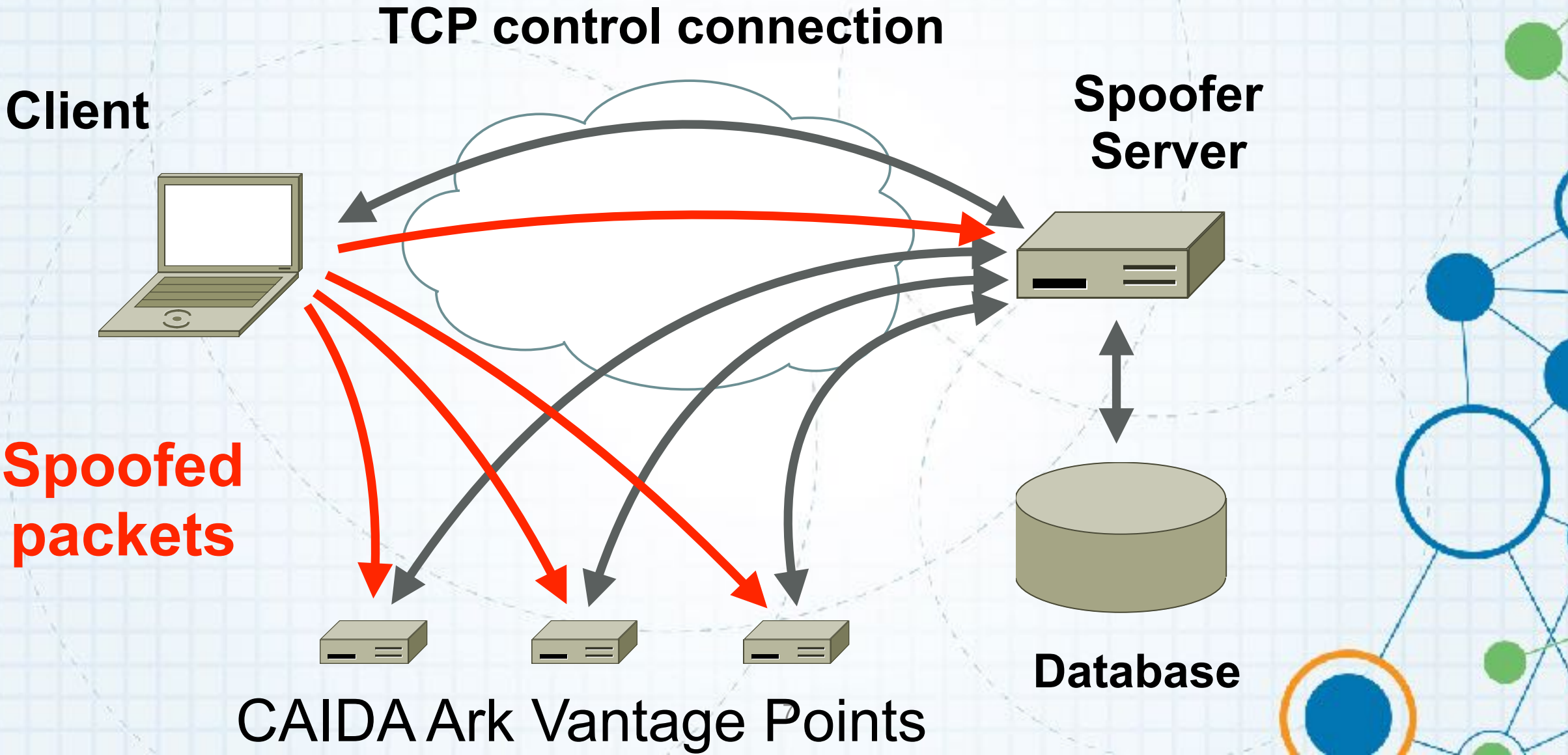
Tragedy of the Commons

- 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 deploy 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 Architecture



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?

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

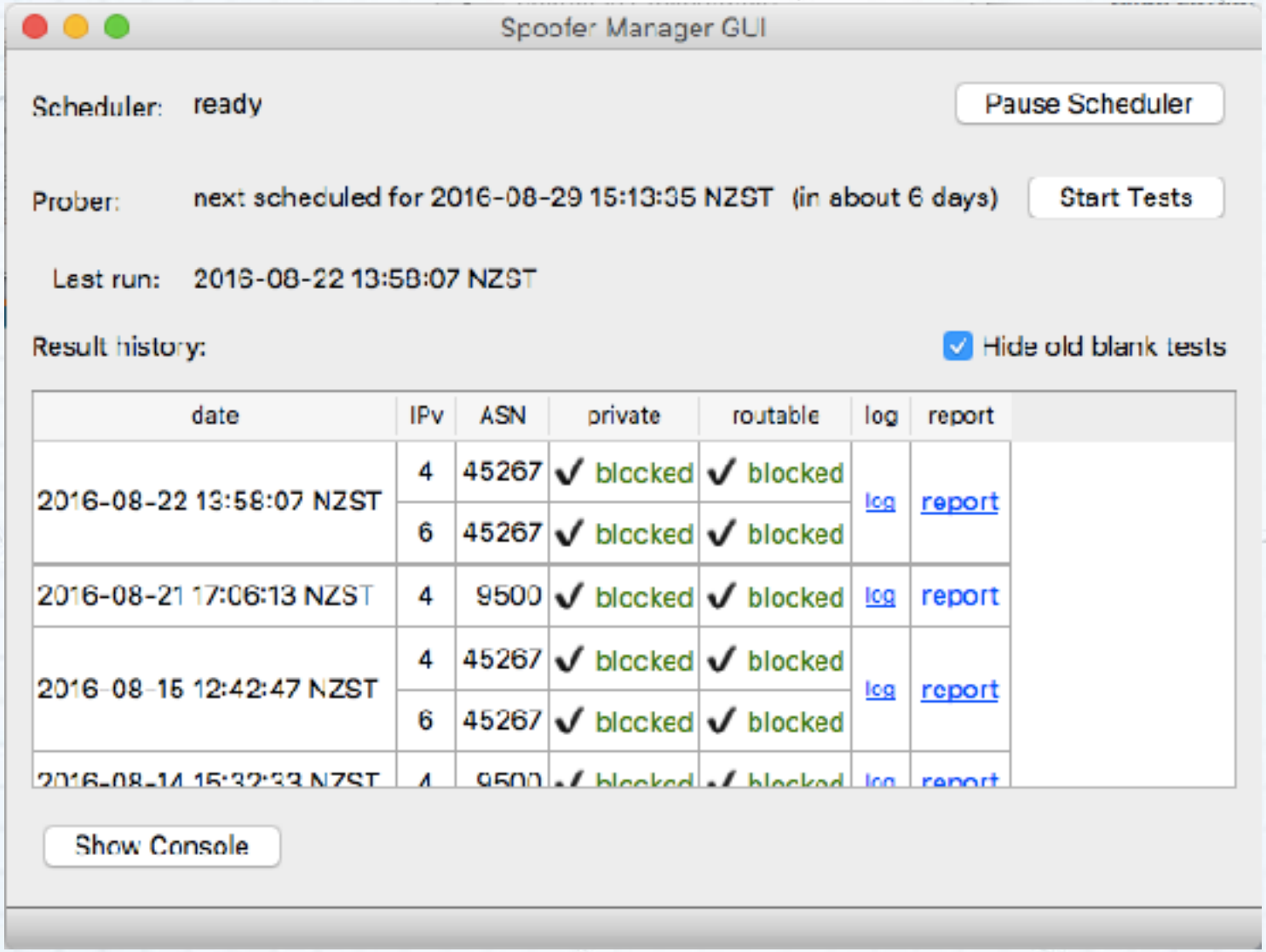
https://spoofer.caida.org/recent_tests.php

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

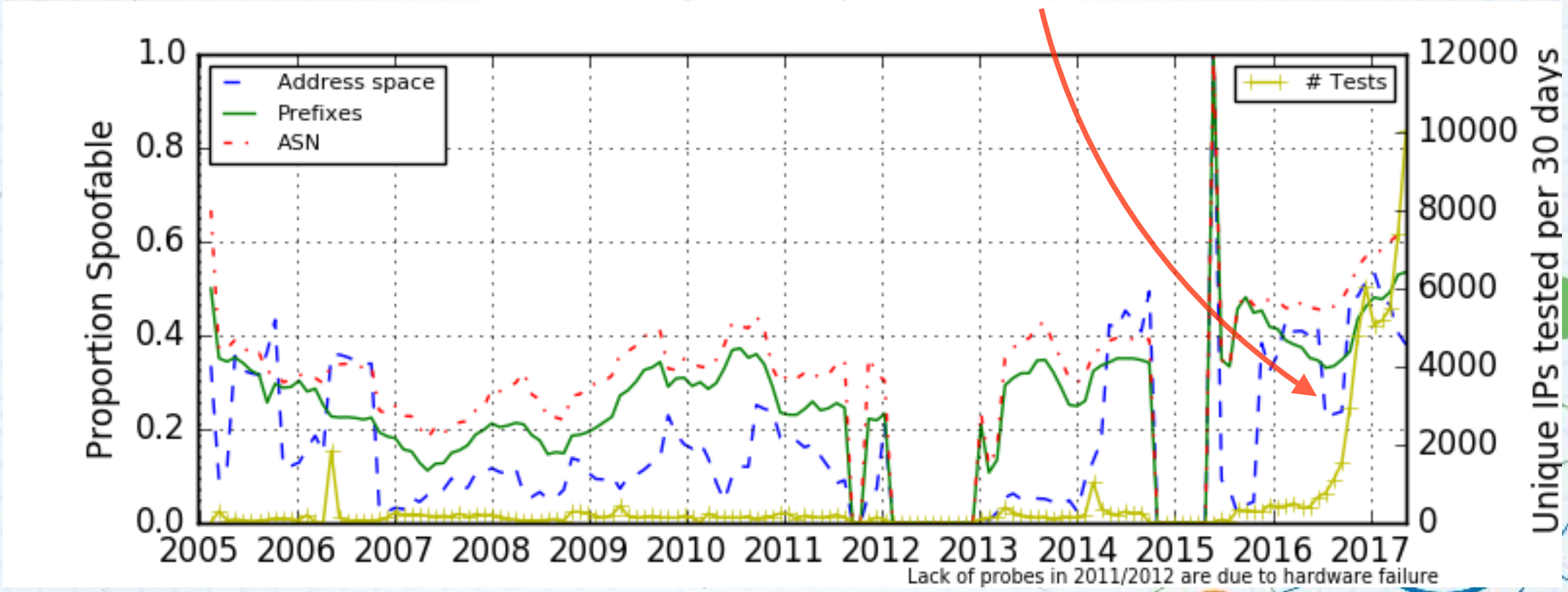
Open Source

C++

Client/Server Deployment

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

Benefit of system running in background



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
		2602:1607: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
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) send (semi-automated) notifications to abuse contacts of prefixes from which we received a spoofed packet.

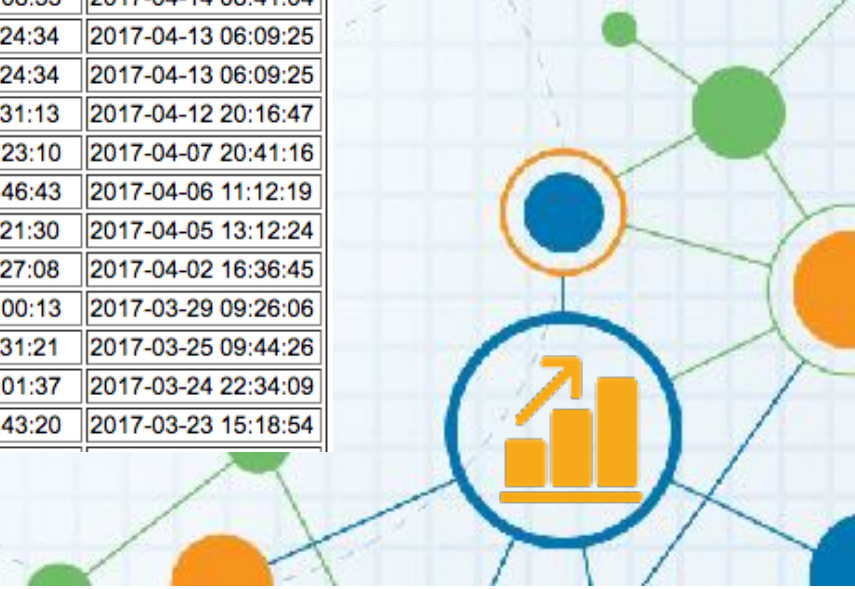
Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 A S	
133390	2017-01-24 19:44:39	182.48.139.x	9245	nzl	no	blocked	blocked	/19	
		2405:8400:10xx::	9245		no	blocked	blocked		
131277	2017-01-17 18:32:55	182.48.139.x	9245	nzl	no	blocked	blocked	/19	
		2405:8400:10xx::	9245		no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

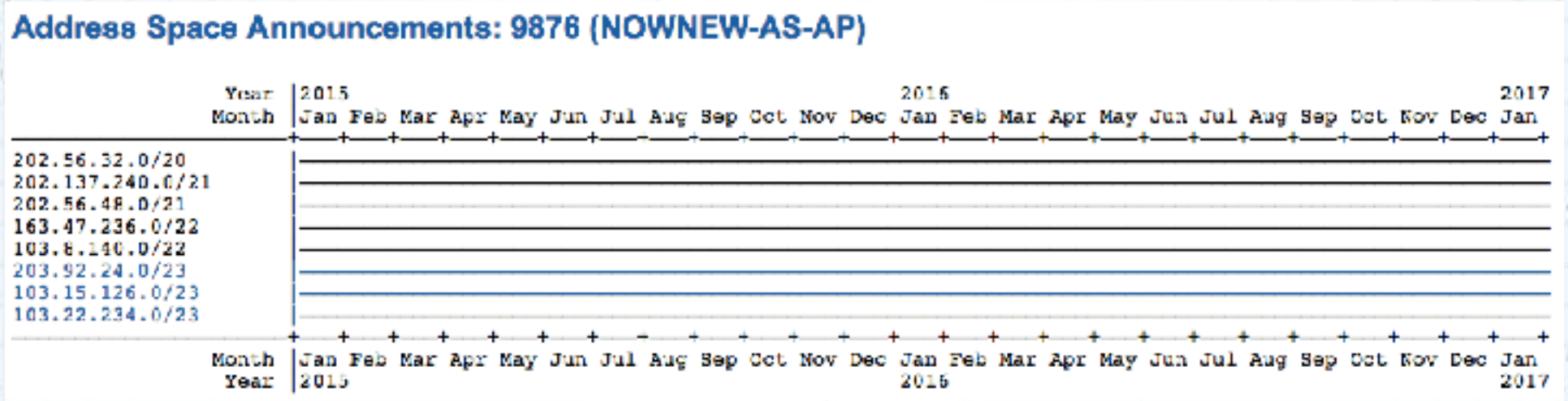
ASN	Country	IP Address	Received Timestamp	Blocked Timestamp
9299 (IPG-AS-AP)	phl (Philippines)	122.52.49.x/24	2017-05-15 19:25:17	2017-05-16 15:30:12
11039 (GWU)	usa (United States)	2620:106:c0xx::/40	2017-05-15 08:36:16	2017-05-16 11:47:20
209 (CENTURYLINK-US-LEGACY-QWEST)	usa (United States)	76.4.117.x/24	2017-05-11 19:40:23	2017-05-15 19:32:58
136301	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)	76.4.126.x/24	2017-05-08 11:17:23	2017-05-08 18:26:16
1653 (SUNET)	swe (Sweden)	193.10.0.x/24	2016-12-15 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 19:16:50
33152 (KCEC-ASN)	usa (United States)	2607:f768:2xx::/40	2017-04-27 09:35:22	2017-04-27 11:46:24
33980 (PAF)	swe (Sweden)	192.165.72.x/24	2017-04-07 12:11:32	2017-04-26 11:04:00
197922 (FIRSTHEBERG)	fra (France)	93.113.206.x/24	2017-04-21 01:56:10	2017-04-23 11:10:15
31857 (PRIORITY-TERABIT)	usa (United States)	69.28.32.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 08:40:02
237 (MERIT-AS-14)	usa (United States)	198.108.63.x/24	2017-02-20 10:39:25	2017-04-18 08:40:02
21804 (ACCESS-SK)	can (Canada)	24.72.6.x/24	2017-02-20 15:08:53	2017-04-14 08:41:04
33980 (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
24211 (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)	198.108.63.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:dc0:a0xx::/40	2016-11-20 20:27:08	2017-04-02 16:36:45
7922 (COMCAST-7922)	usa (United States)	2601:601:80xx::/40	2017-03-21 22:00:13	2017-03-29 09:26:06
394437 (PSLIGHTWAVE)	usa (United States)	2606:a780:xx::/40	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

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

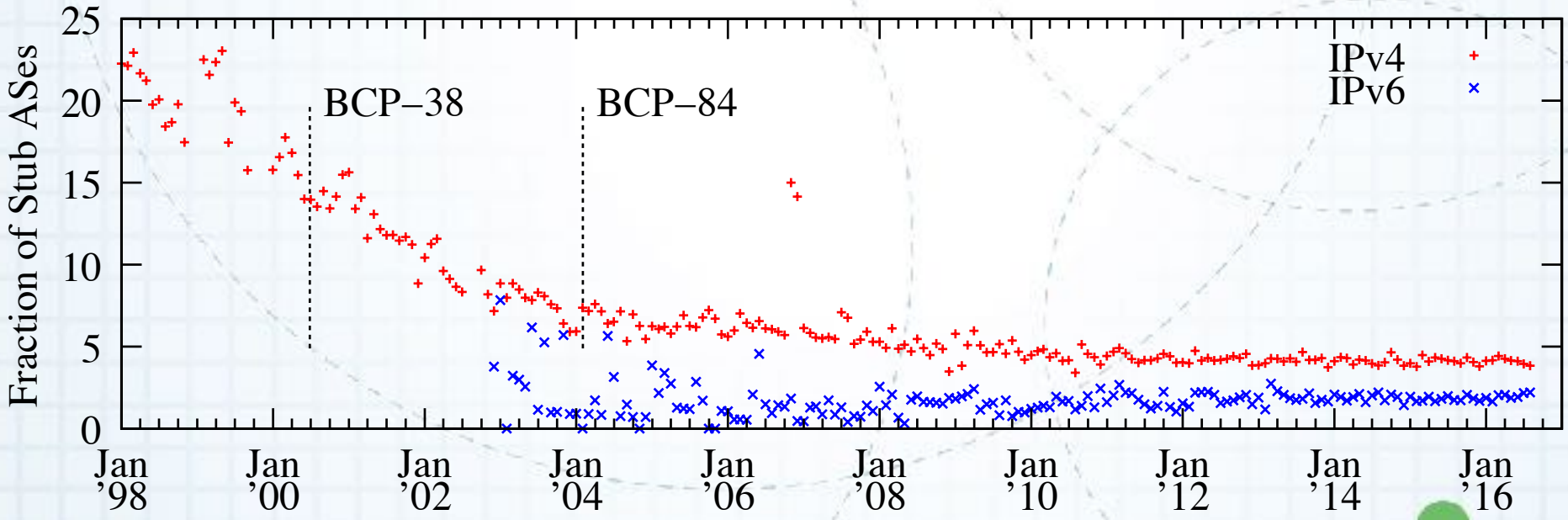
https://spoofer.caida.org/provider.php

[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.

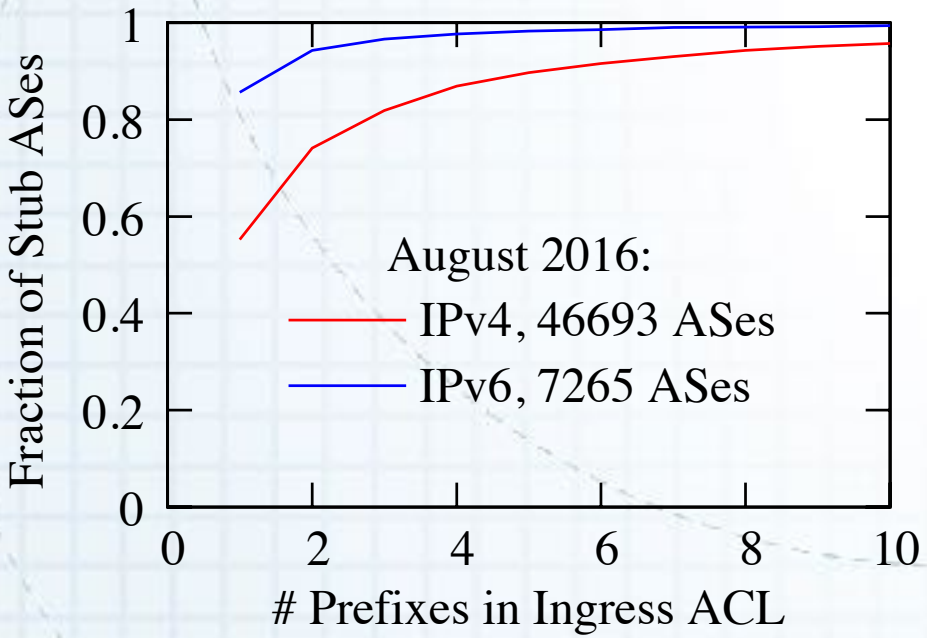


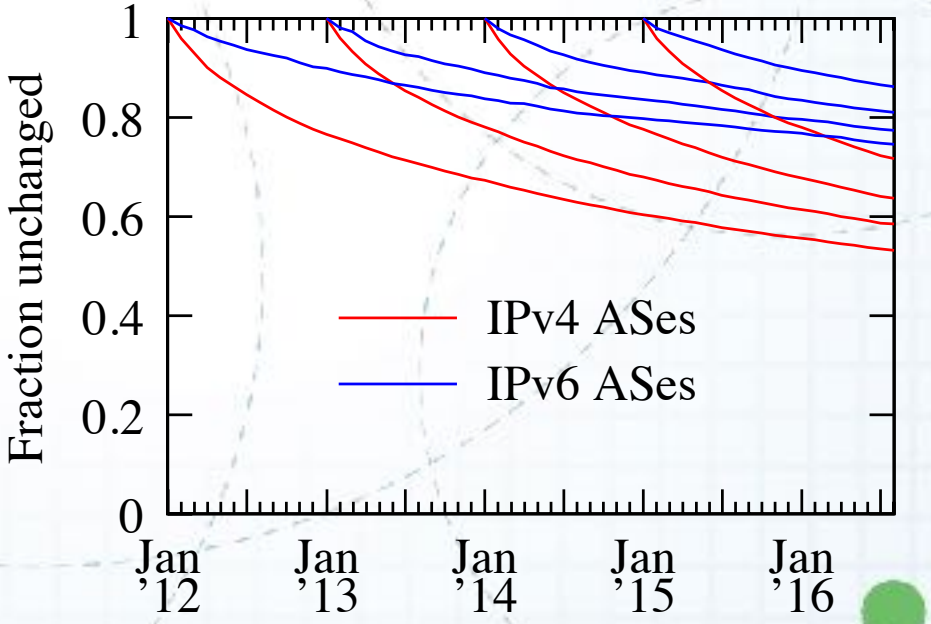
Data Source: Routeviews and RIPE RIS data

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.

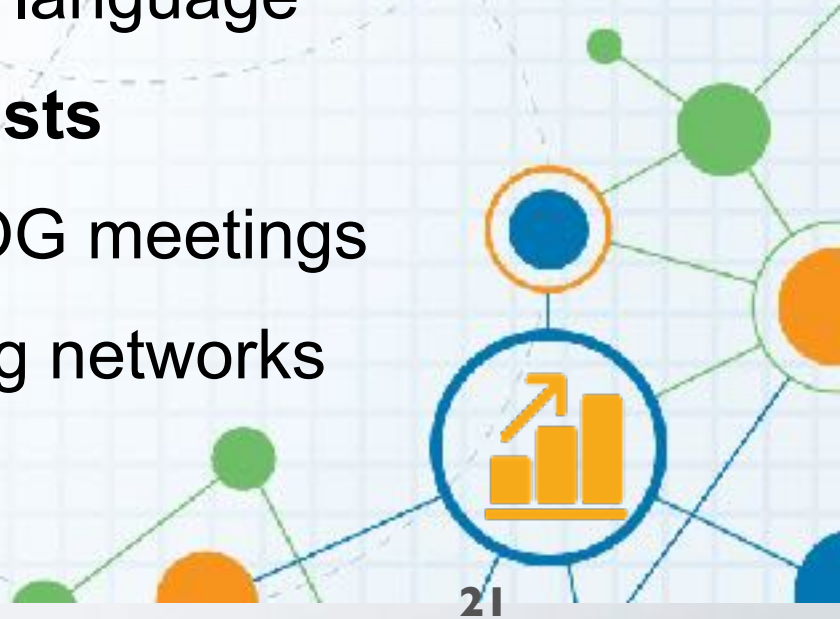




Data Source: Routeviews and RIPE RIS data

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
  - Next step: hall of shame/fame



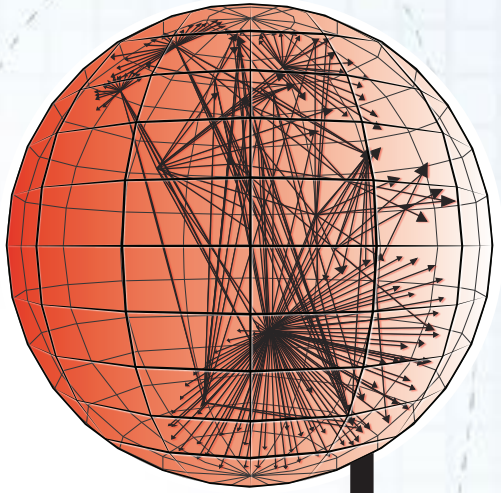
Should I install the client?

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

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

2017 Cyber Security R&D Showcase and Technical Workshop

July 11 - 13, 2017 | Washington, D.C.

Homeland Security

Science and Technology