Homeland Security
Science and Technology

2016 | Cyber Security Division

DDoSD Principal Investigator Meeting

Software Systems for Surveying Spoofing Susceptibility

CAIDA / UC San Diego

Matthew Luckie (U. Waikato)

August 1st, 2016

Team Profile

The Center for Applied Internet Data Analysis (CAIDA)

- Founded by PI and Director k claffy
- Independent analysis and research group
- 15+ years experience in data collection, curation, and research
- Renowned world-wide for data collection tools, analysis, and data sharing
- Located at the University of California's San Diego Supercomputer Center

Key spoofer personnel: k claffy, Matthew Luckie, Ken Keys, Ryan Koga, Bradley Huffaker, Alberto Dainotti, Daniel Anderson, Robert Beverly

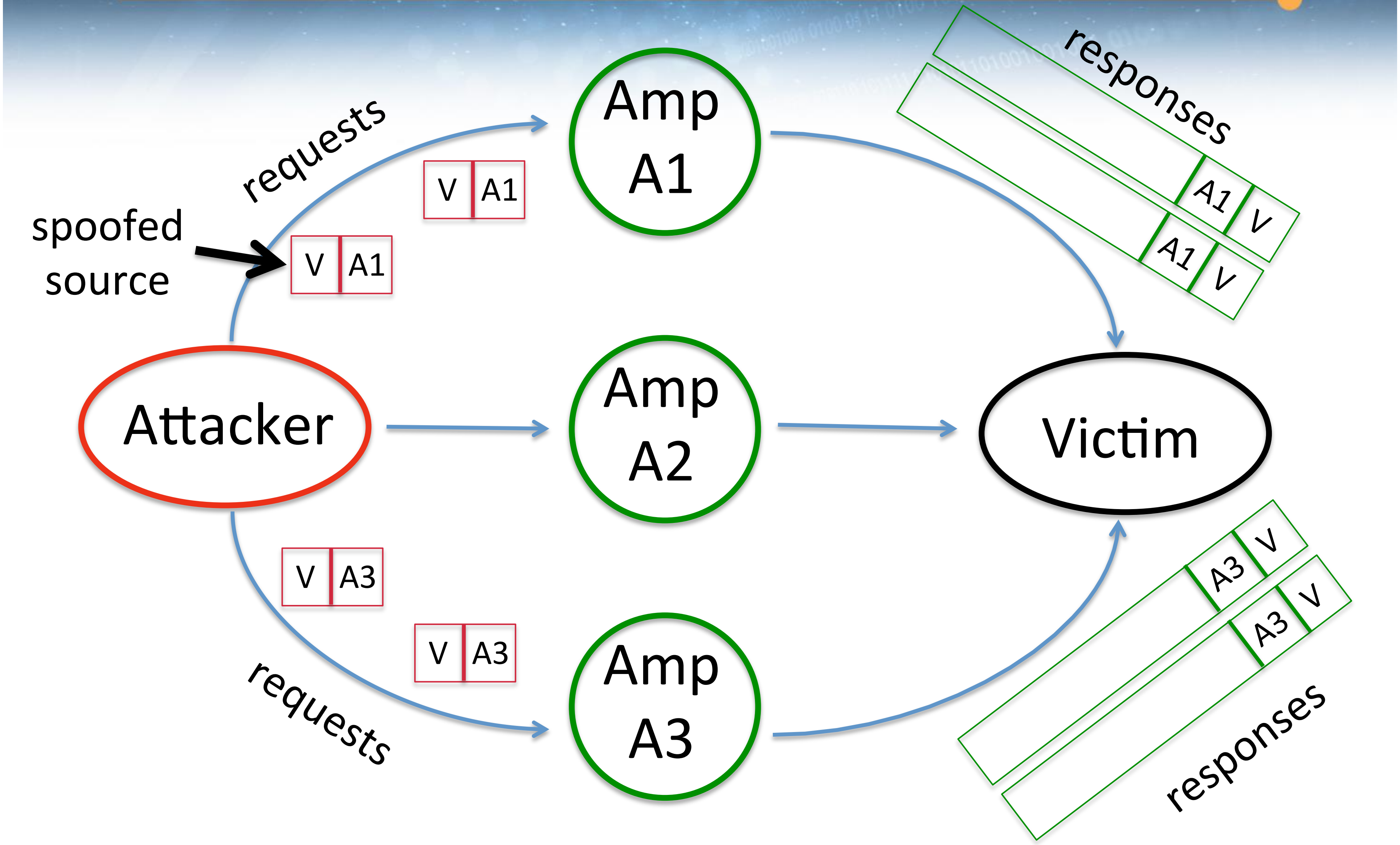
Project Description

Develop, test, and deploy new tools to measure and report on the deployment of source address validation (SAV) best practices – “anti-spoofing”

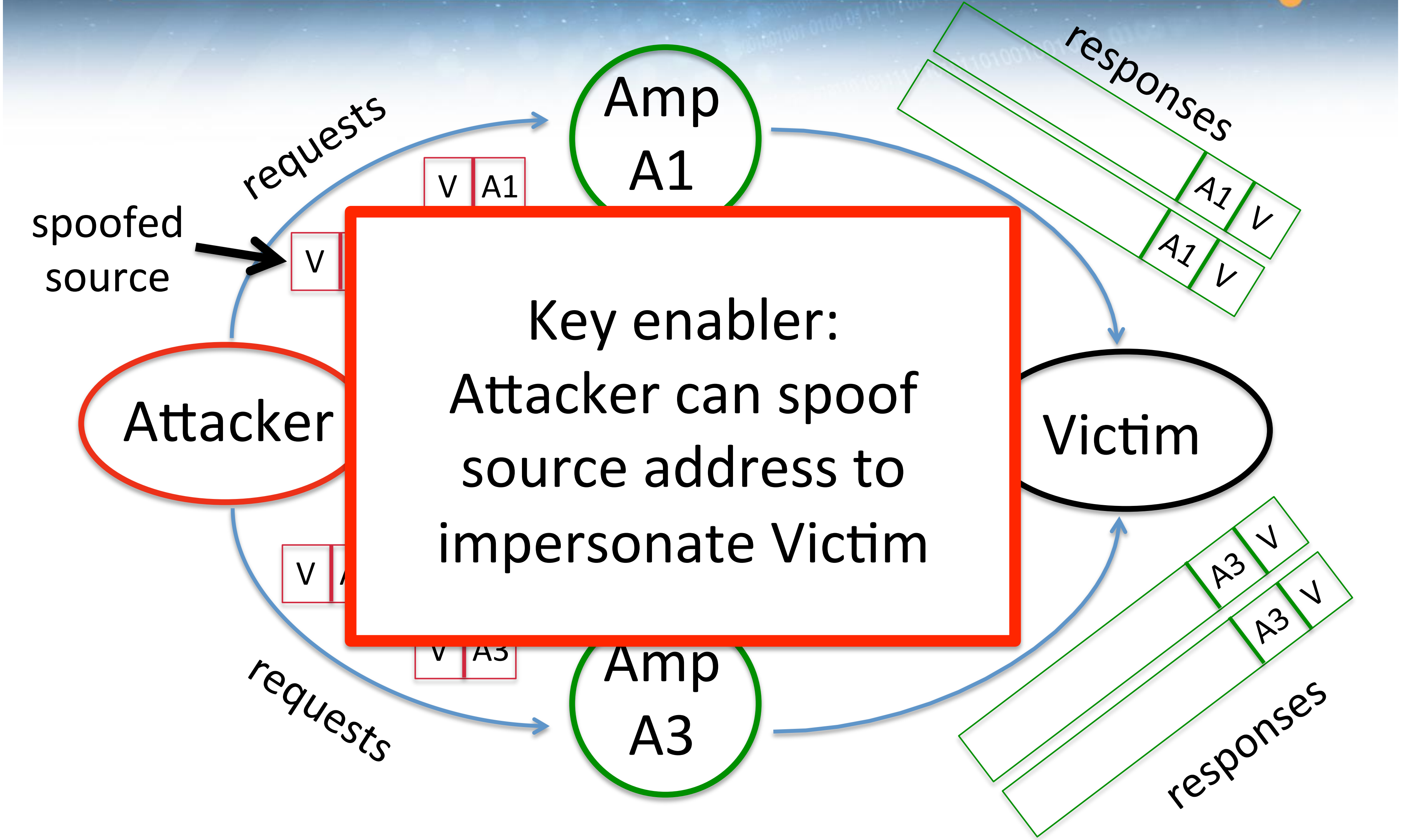
- BCP38: Network ingress filtering: defeating denial of service attacks which employ IP Source Address Spoofing
  - http://tools.ietf.org/html/bcp38
- BCP84: Ingress filtering for multi-homed networks
  - http://tools.ietf.org/html/bcp84

Not always straight forward to deploy

Amplification DoS Attack



Amplification DoS Attack



Key enabler:
Attacker can spoof source address to impersonate Victim

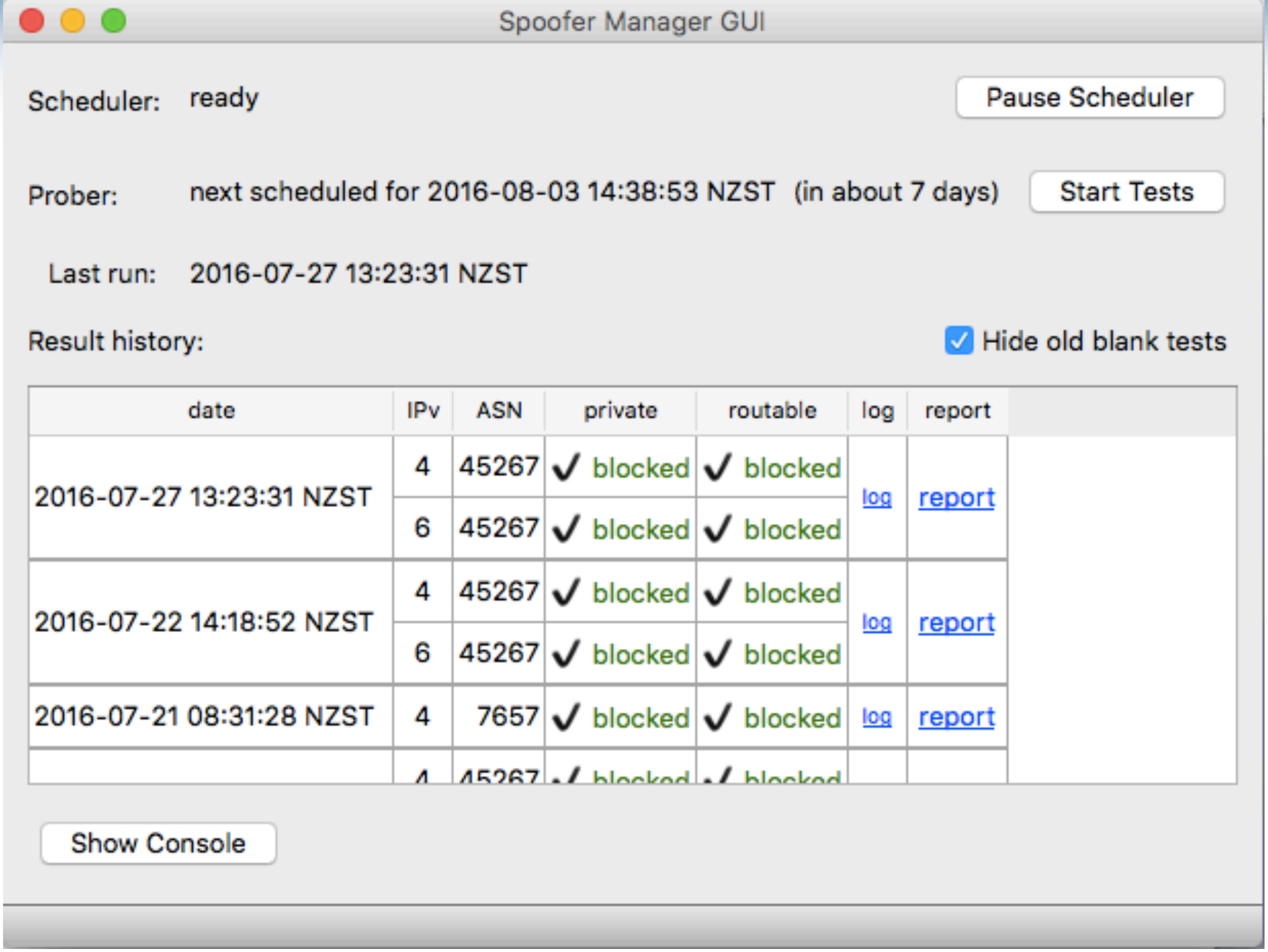
Customer Need

- No public view of exactly which networks have not deployed SAV
- To solve this problem, DHS needs:
  - ❑ A production-quality SAV testing system
  - ❑ A topology-analysis system to identify transit ASes that do not filter customer ASes
  - ❑ Data analysis to inform assessment of infrastructure hygiene and effectiveness of anti-spoofing efforts

Approach: client-server

- Develop, test, and deploy a production-quality system to measure deployment of SAV
  - ❑ New GUI-based client/server testing system
  - ❑ User incentives for persistent deployment
  - ❑ Opt-in to share anonymised results of tests to provide public view
  - ❑ Opt-in to share unanonymised results of tests for remediation purposes
  - ❑ Cross platform: MacOS, Windows, Linux, BSD.
- New system collects data automatically, once a week, and whenever attached to a new network

Approach: client-server



Spoofer Manager GUI

Scheduler: ready

Prober: next scheduled for 2016-08-03 14:38:53 NZST (in about 7 days)

Last run: 2016-07-27 13:23:31 NZST

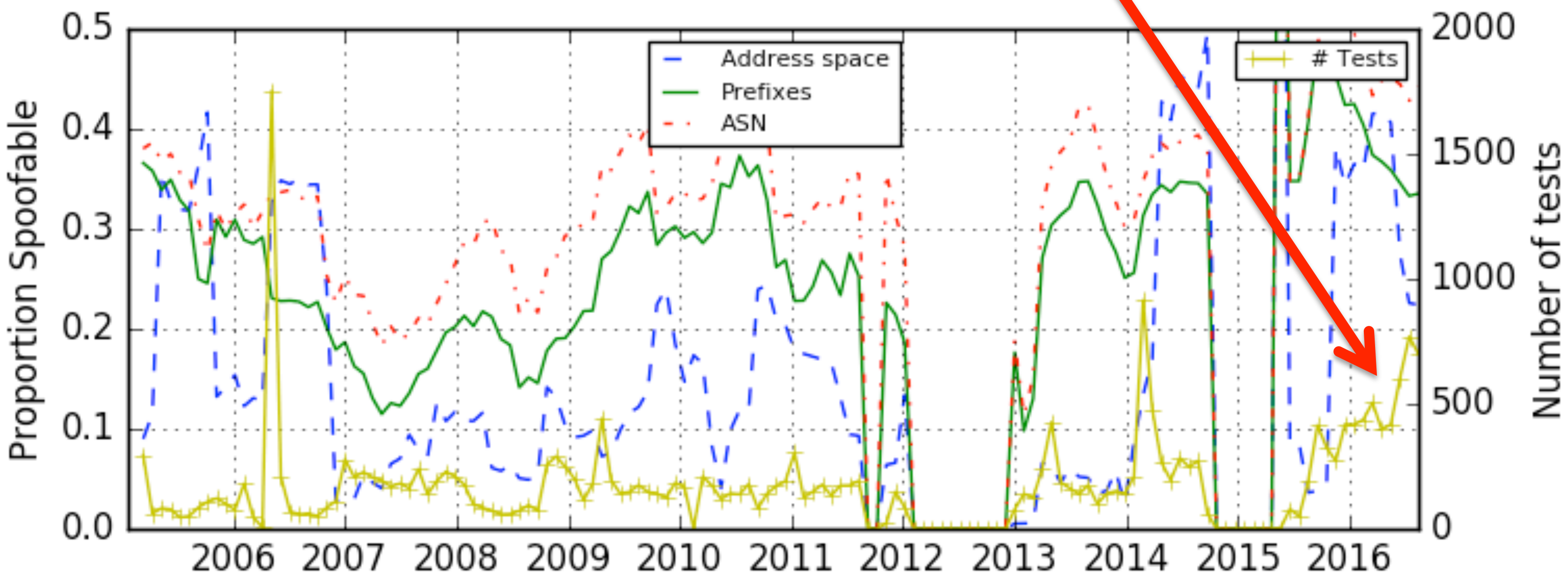
Result history:

☑ Hide old blank tests

date	IPv	ASN	private	routable	log	report
2016-07-27 13:23:31 NZST	4	45267	✓ blocked	✓ blocked	log	report
	6	45267	✓ blocked	✓ blocked		
2016-07-22 14:18:52 NZST	4	45267	✓ blocked	✓ blocked	log	report
	6	45267	✓ blocked	✓ blocked		
2016-07-21 08:31:28 NZST	4	7657	✓ blocked	✓ blocked	log	report
	4	45267	✓ blocked	✓ blocked		

Approach: client-server

- Since releasing new client in May, six-month trend of more tests is increasing (yellow line)
  - Benefit of client system running unobtrusively in background
  - Haven’t started deployment push yet



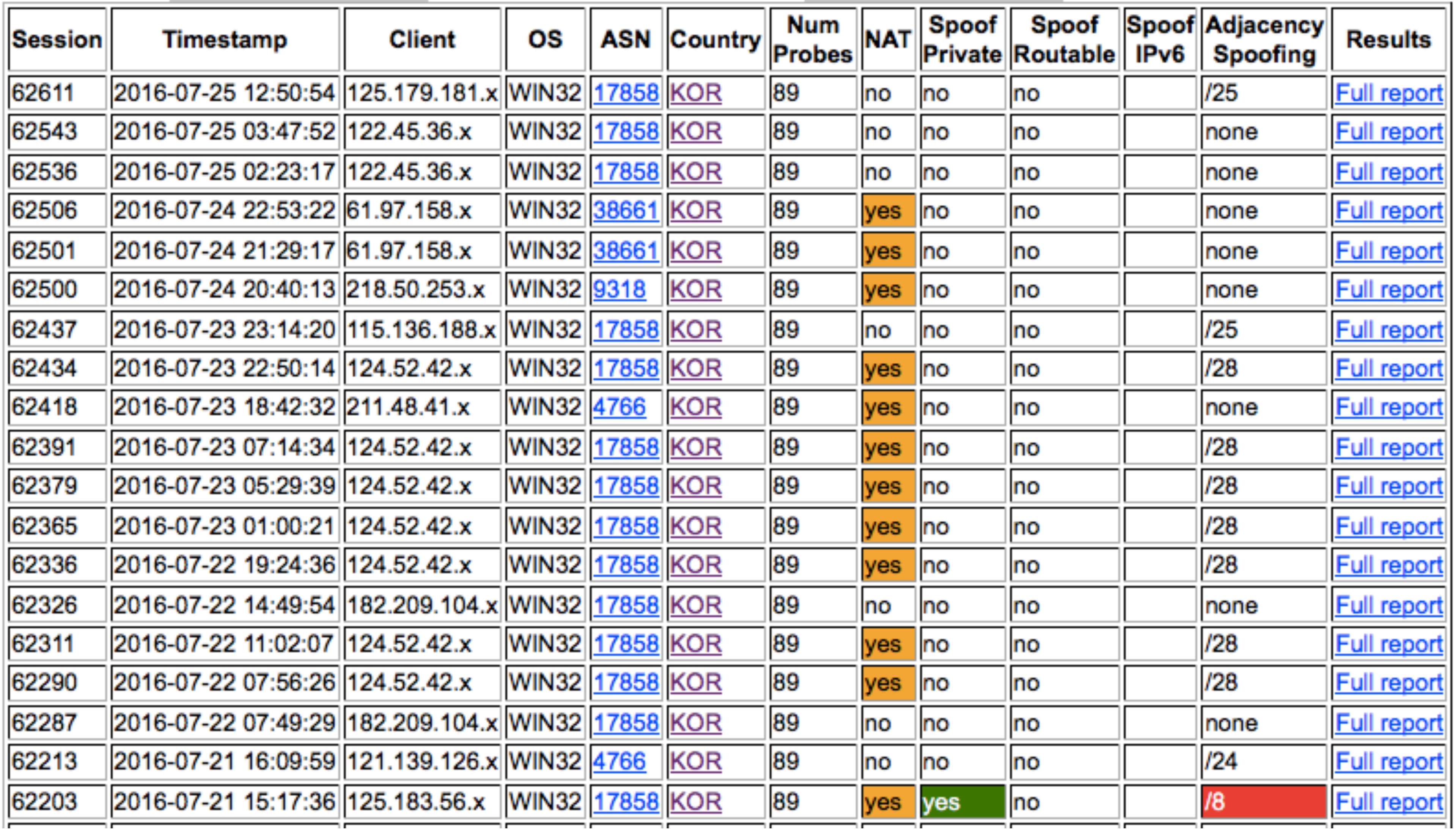
Lack of probes in 2011/2012 are due to hardware failure

Approach: reporting engine

- Deliver public reports that assess and promote deployment of SAV
  - ❑ Per-country analysis of tests at country granularity
  - ❑ Per-country analysis of tests at AS-level granularity
  - ❑ Transit provider view of customer ASes: which customers have not deployed SAV?
  - ❑ Correlate SAV measurements with characteristics of network types: access, transit, reputation
  - ❑ Automatically report outcomes of tests to network operators via abuse contact information

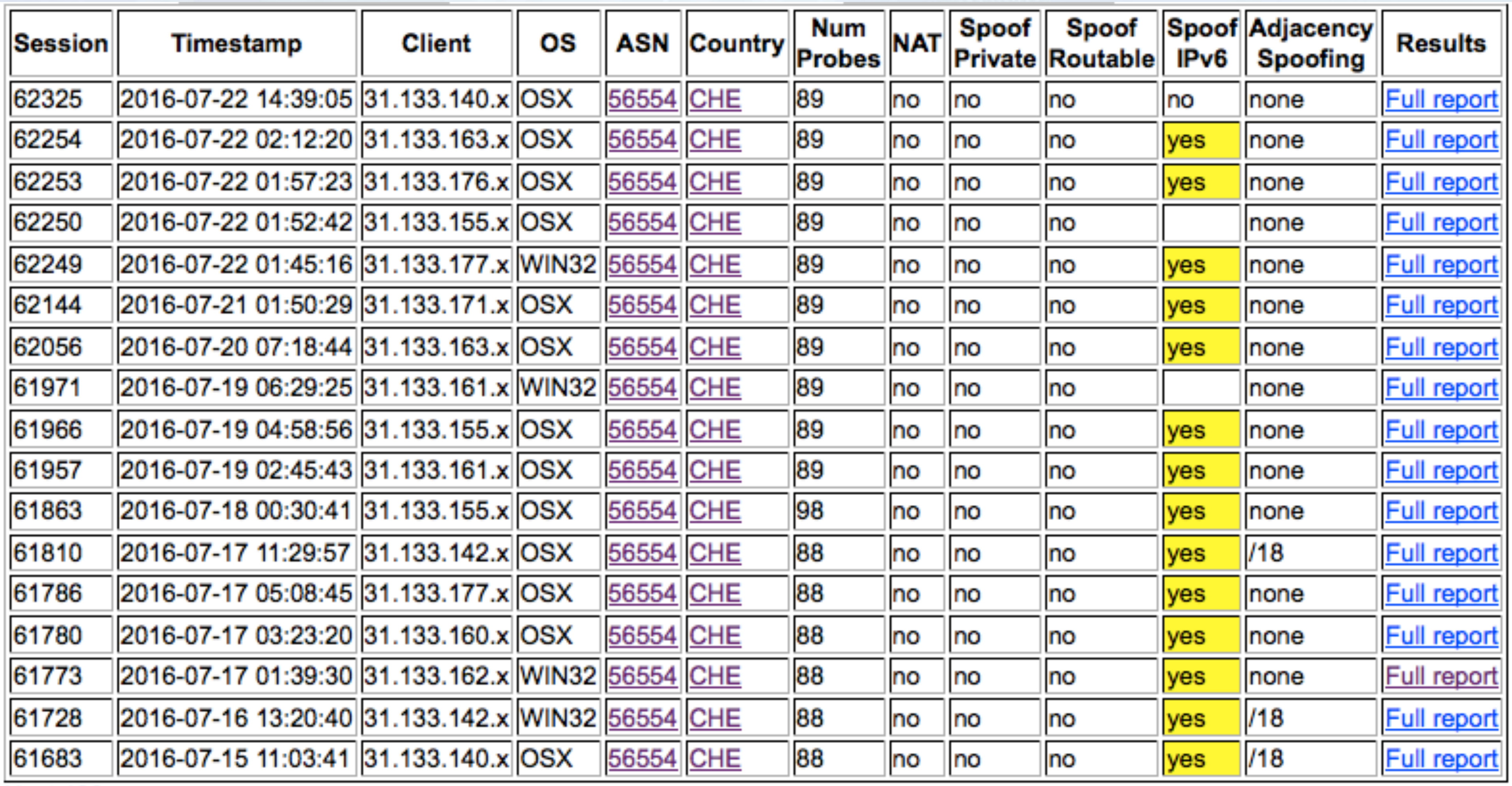
https://spoofer.caida.org/recent_tests.php

Approach: reporting engine



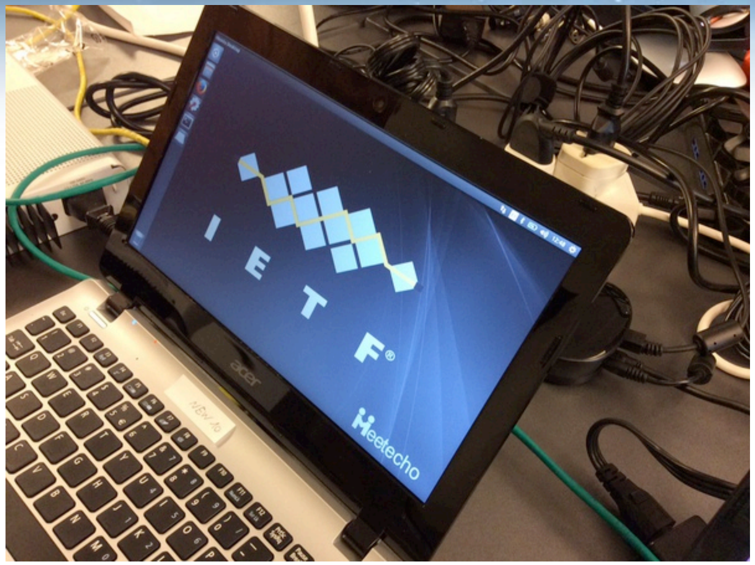
Session	Timestamp	Client	OS	ASN	Country	Num Probes	NAT	Spoof Private	Spoof Routable	Spoof IPv6	Adjacency Spoofing	Results
62611	2016-07-25 12:50:54	125.179.181.x	WIN32	17858	KOR	89	no	no	no		/25	Full report
62543	2016-07-25 03:47:52	122.45.36.x	WIN32	17858	KOR	89	no	no	no		none	Full report
62536	2016-07-25 02:23:17	122.45.36.x	WIN32	17858	KOR	89	no	no	no		none	Full report
62506	2016-07-24 22:53:22	61.97.158.x	WIN32	38661	KOR	89	yes	no	no		none	Full report
62501	2016-07-24 21:29:17	61.97.158.x	WIN32	38661	KOR	89	yes	no	no		none	Full report
62500	2016-07-24 20:40:13	218.50.253.x	WIN32	9318	KOR	89	yes	no	no		none	Full report
62437	2016-07-23 23:14:20	115.136.188.x	WIN32	17858	KOR	89	no	no	no		/25	Full report
62434	2016-07-23 22:50:14	124.52.42.x	WIN32	17858	KOR	89	yes	no	no		/28	Full report
62418	2016-07-23 18:42:32	211.48.41.x	WIN32	4766	KOR	89	yes	no	no		none	Full report
62391	2016-07-23 07:14:34	124.52.42.x	WIN32	17858	KOR	89	yes	no	no		/28	Full report
62379	2016-07-23 05:29:39	124.52.42.x	WIN32	17858	KOR	89	yes	no	no		/28	Full report
62365	2016-07-23 01:00:21	124.52.42.x	WIN32	17858	KOR	89	yes	no	no		/28	Full report
62336	2016-07-22 19:24:36	124.52.42.x	WIN32	17858	KOR	89	yes	no	no		/28	Full report
62326	2016-07-22 14:49:54	182.209.104.x	WIN32	17858	KOR	89	no	no	no		none	Full report
62311	2016-07-22 11:02:07	124.52.42.x	WIN32	17858	KOR	89	yes	no	no		/28	Full report
62290	2016-07-22 07:56:26	124.52.42.x	WIN32	17858	KOR	89	yes	no	no		/28	Full report
62287	2016-07-22 07:49:29	182.209.104.x	WIN32	17858	KOR	89	no	no	no		none	Full report
62213	2016-07-21 16:09:59	121.139.126.x	WIN32	4766	KOR	89	no	no	no		/24	Full report
62203	2016-07-21 15:17:36	125.183.56.x	WIN32	17858	KOR	89	yes	yes	no		/8	Full report

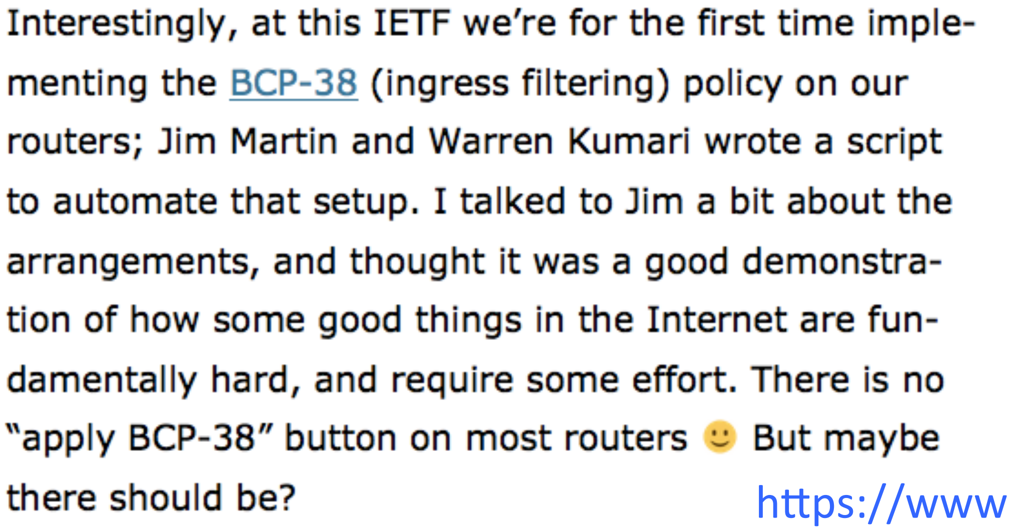
Approach: reporting engine



Session	Timestamp	Client	OS	ASN	Country	Num Probes	NAT	Spoof Private	Spoof Routable	Spoof IPv6	Adjacency Spoofing	Results
62325	2016-07-22 14:39:05	31.133.140.x	OSX	56554	CHE	89	no	no	no	no	none	Full report
62254	2016-07-22 02:12:20	31.133.163.x	OSX	56554	CHE	89	no	no	no	yes	none	Full report
62253	2016-07-22 01:57:23	31.133.176.x	OSX	56554	CHE	89	no	no	no	yes	none	Full report
62250	2016-07-22 01:52:42	31.133.155.x	OSX	56554	CHE	89	no	no	no		none	Full report
62249	2016-07-22 01:45:16	31.133.177.x	WIN32	56554	CHE	89	no	no	no	yes	none	Full report
62144	2016-07-21 01:50:29	31.133.171.x	OSX	56554	CHE	89	no	no	no	yes	none	Full report
62056	2016-07-20 07:18:44	31.133.163.x	OSX	56554	CHE	89	no	no	no	yes	none	Full report
61971	2016-07-19 06:29:25	31.133.161.x	WIN32	56554	CHE	89	no	no	no		none	Full report
61966	2016-07-19 04:58:56	31.133.155.x	OSX	56554	CHE	89	no	no	no	yes	none	Full report
61957	2016-07-19 02:45:43	31.133.161.x	OSX	56554	CHE	89	no	no	no	yes	none	Full report
61863	2016-07-18 00:30:41	31.133.155.x	OSX	56554	CHE	98	no	no	no	yes	none	Full report
61810	2016-07-17 11:29:57	31.133.142.x	OSX	56554	CHE	88	no	no	no	yes	/18	Full report
61786	2016-07-17 05:08:45	31.133.177.x	OSX	56554	CHE	88	no	no	no	yes	none	Full report
61780	2016-07-17 03:23:20	31.133.160.x	OSX	56554	CHE	88	no	no	no	yes	none	Full report
61773	2016-07-17 01:39:30	31.133.162.x	WIN32	56554	CHE	88	no	no	no	yes	none	Full report
61728	2016-07-16 13:20:40	31.133.142.x	WIN32	56554	CHE	88	no	no	no	yes	/18	Full report
61683	2016-07-15 11:03:41	31.133.140.x	OSX	56554	CHE	88	no	no	no	yes	/18	Full report

Approach: reporting engine





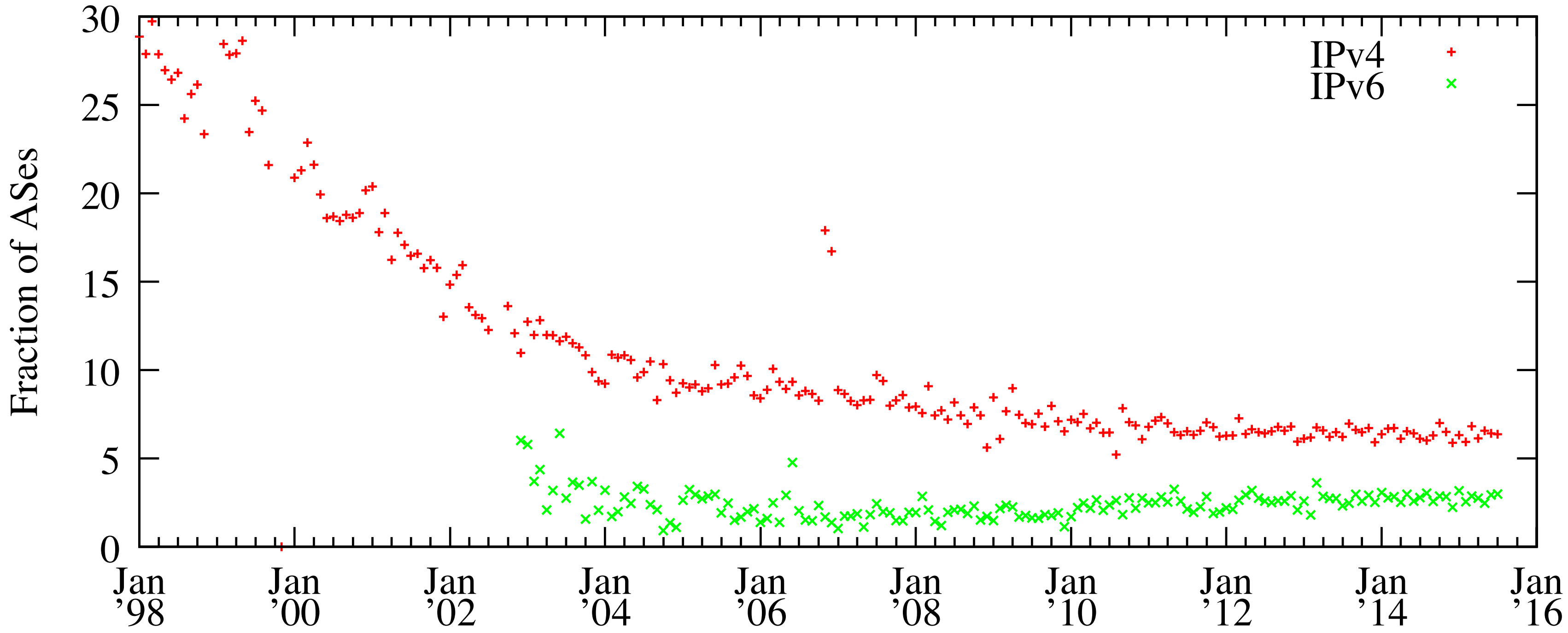
Interestingly, at this IETF we're for the first time implementing the BCP-38 (ingress filtering) policy on our routers; Jim Martin and Warren Kumari wrote a script to automate that setup. I talked to Jim a bit about the arrangements, and thought it was a good demonstration of how some good things in the Internet are fundamentally hard, and require some effort. There is no "apply BCP-38" button on most routers 🙂 But maybe there should be?

Client and reporting system help validate deployment of SAV

https://www.ietf.org/blog/2016/07/berlin-network/

Approach: ingress access lists

During 2016, ~6% and ~3% of ASes announced different IPv4 and IPv6 address space month-to-month, respectively. Increased stability in addressing may make it feasible to use static ingress access lists.



Source: Routeviews and RIPE RIS BGP Data

Approach: customer cones

- Evaluated whether or not customer cones inferred from public BGP data could predict source addresses observed at Anycast DNS instances
  - DITL 2015 – packet captures and routing tables
- Worked well: 97% of addresses from inferred ranges for 24 of 47 instances

Benefits

- Measurement platform to test SAV compliance
- Strategies for mitigating susceptibility to DDoS attacks that are a threat to national security, commerce, and critical infrastructure
- Software tools that use open source licenses
- Data publicly available
  - https://spoofer.caida.org/
- Project targets BAA TTA #1 goal of focusing BCP38 compliance attention where it will most benefit

Contact Information

Matthew Luckie
University of Waikato
mjl@wand.net.nz

Kimberly Claffy
CAIDA / UC San Diego
kc@caida.org