Homeland Security

Science and Technology

SECURING YOUR CYBER FUTURE

2016 | Cyber Security Division

R&D SHOWCASE AND TECHNICAL WORKSHOP

February 17–19, 2016

Washington, DC

Homeland Security
Science and Technology

2016 | Cyber Security Division
R&D SHOWCASE AND TECHNICAL WORKSHOP

TTA 1: Software Systems for Surveying Spoofing Susceptibility

CAIDA/UCSD
PI kc claffy @ UCSD
in collaboration with
Professor Matthew Luckie @ U. Waikato
and Professor Robert Beverly @ NPS

17-19 February 2016

Team Profile

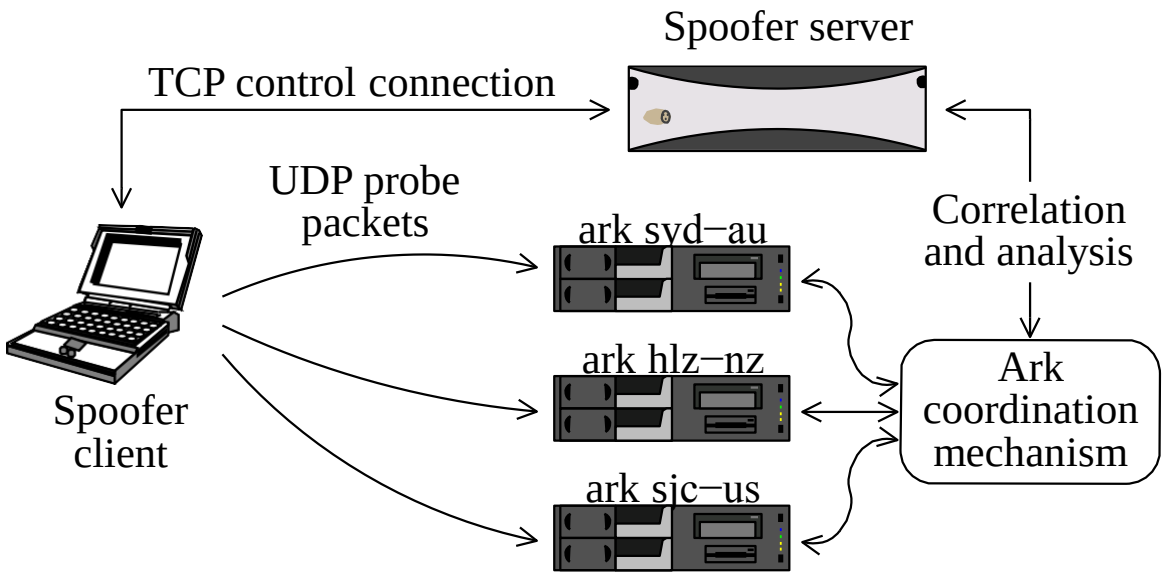
The Center for Applied Internet Data Analysis (CAIDA)

- –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 personnel: **kc claffy, Matthew Luckie,** Ken Keys, Daniel Anderson, Alberto Dainotti

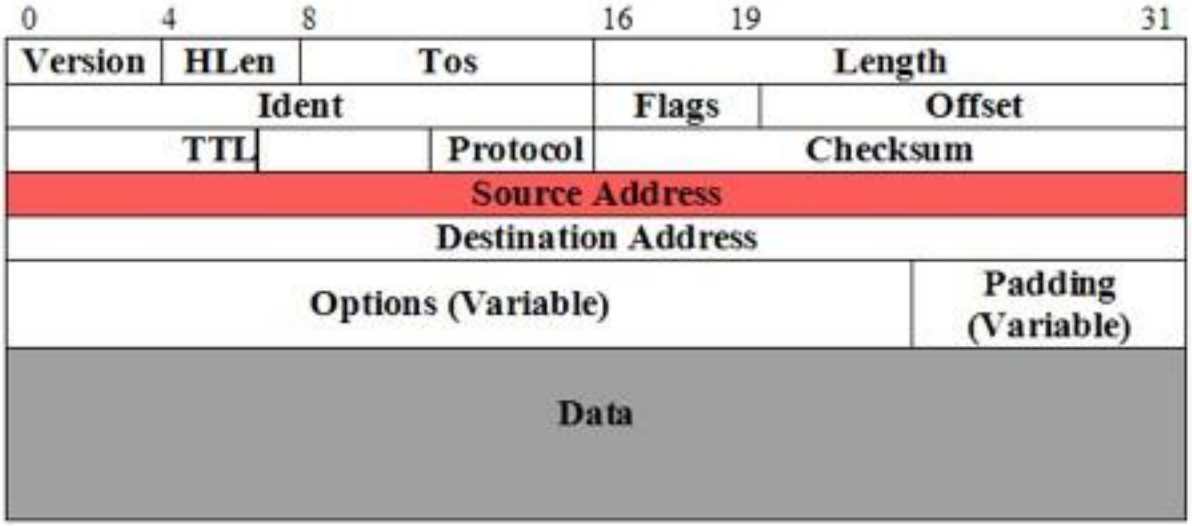
Project Description

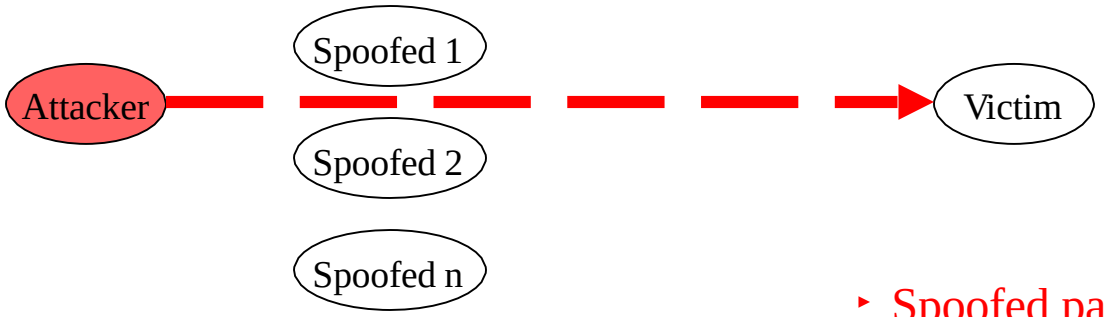
Develop, test and deploy new tools to measure and report on the deployment of source address validation (SAV) best practices (anti-“spoofing” filtering).



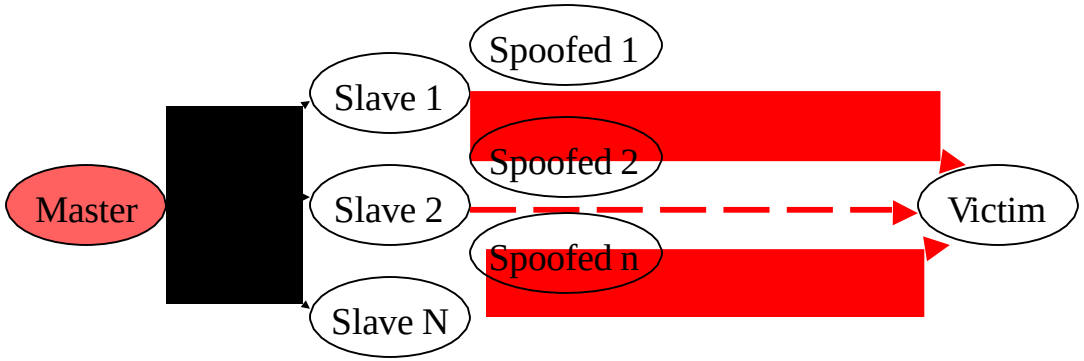
What are spoofed packets?

- Attackers/compromised-hosts forge or “spoof” source address of an IP packet
- Trivially done at host

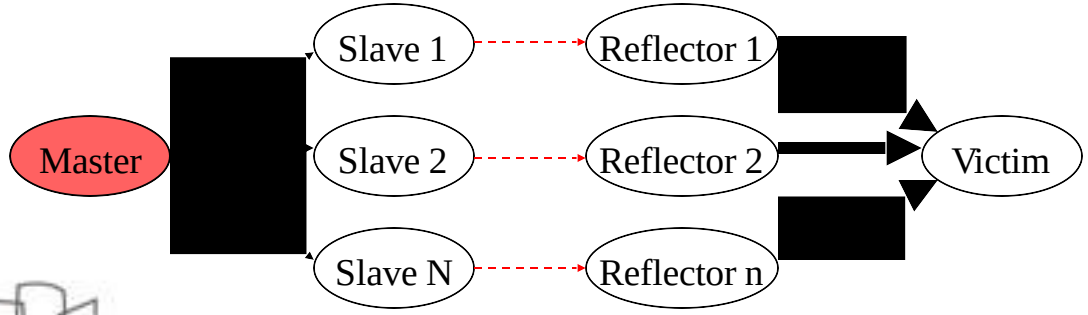




DoS attack with spoofing



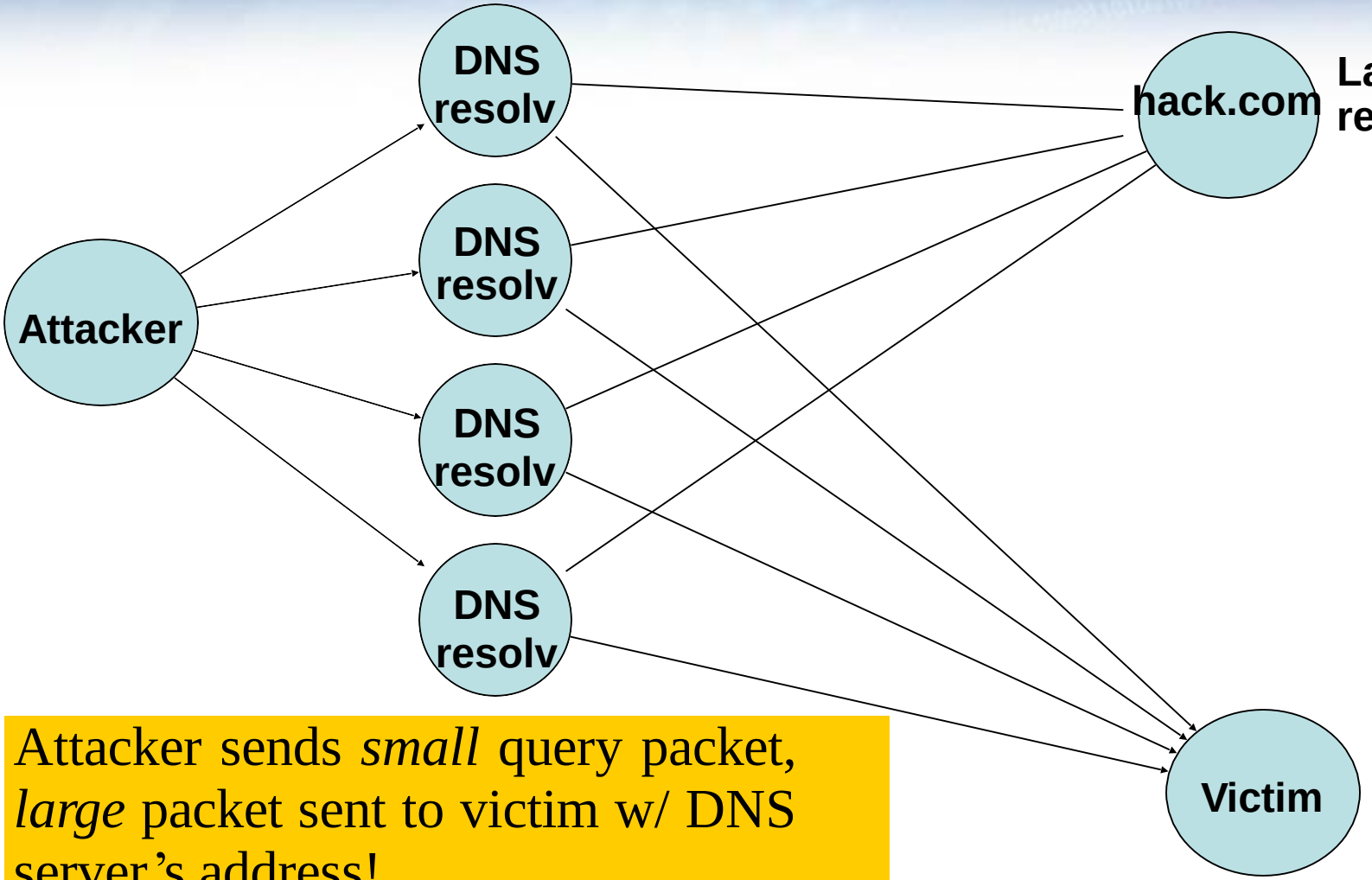
Distributed DoS attack with spoofing



Distributed DoS attack with reflectors

CSAIL

DNS Reflector + Amplification Attack

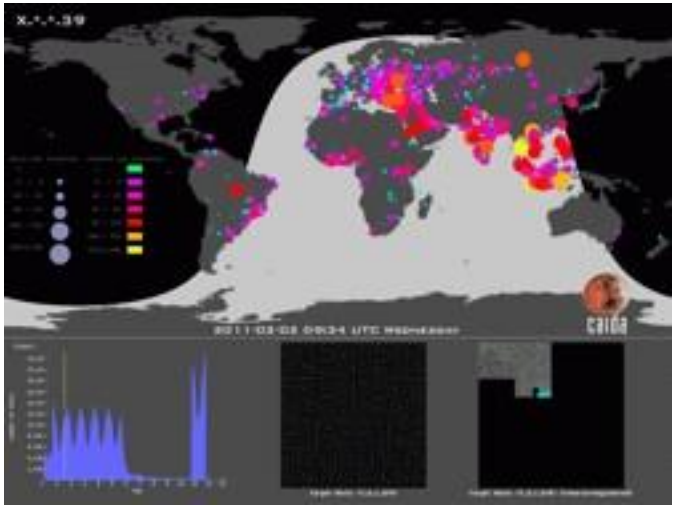


Attacker sends *small* query packet, *large* packet sent to victim w/ DNS server's address!

BCP 38 / 84 - Ingress Filtering

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (http://tools.ietf.org/html/bcp38)

Ingress Filtering for Multihomed Networks (http://tools.ietf.org/html/bcp84)



[Customer] Need

Spoofing Threat

Many ISPs provide (that is, do not filter) transit of IP packets with forged source addresses in the packet headers. This lack of filtering facilitates anonymous perpetration of Denial-of-Service (DDoS) attacks, since it renders it complex and expensive to discover the source of an attack.

To solve this problem, DHS needs:

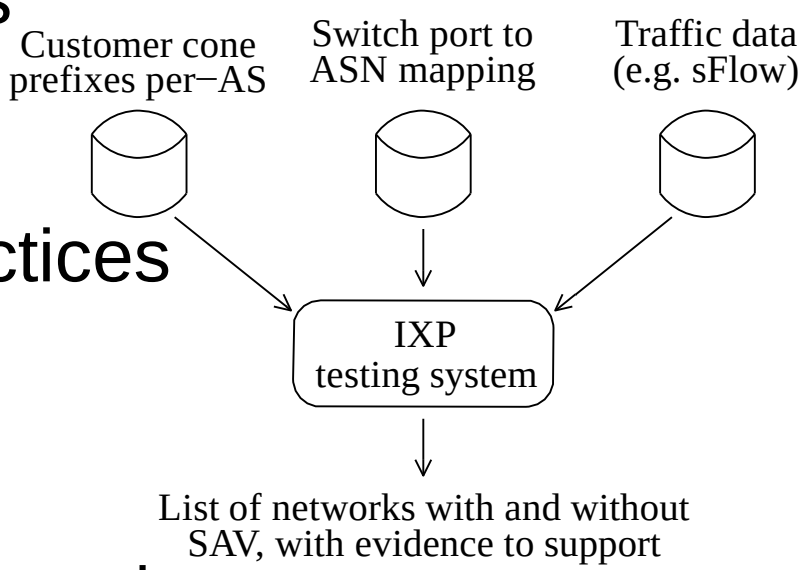
- a production-quality SAV testing system;
- data analysis to inform assessment of infrastructure hygiene and effectiveness of anti-spoofing compliance efforts
- a traffic analysis system to infer evidence of whether ASes participating at IXPs have deployed SAV best practices

Approach

- Develop, test, and deploy a production-quality system and tools to measure and report on the deployment of source address validation (SAV)
  - new client/server testing system
  - user incentives for persistent deployment
- Deliver reports to assess and promote deployment of anti-spoofing best practices
  - correlate SAV measurements with characteristics of network type (e.g., access, transit, reputation)
  - per-country analysis of transit provider SAV compliance
  - experiment with and evaluate effectiveness of reporting mechanisms, e.g., periodically updated web pages, email to network contacts, Twitter

Approach

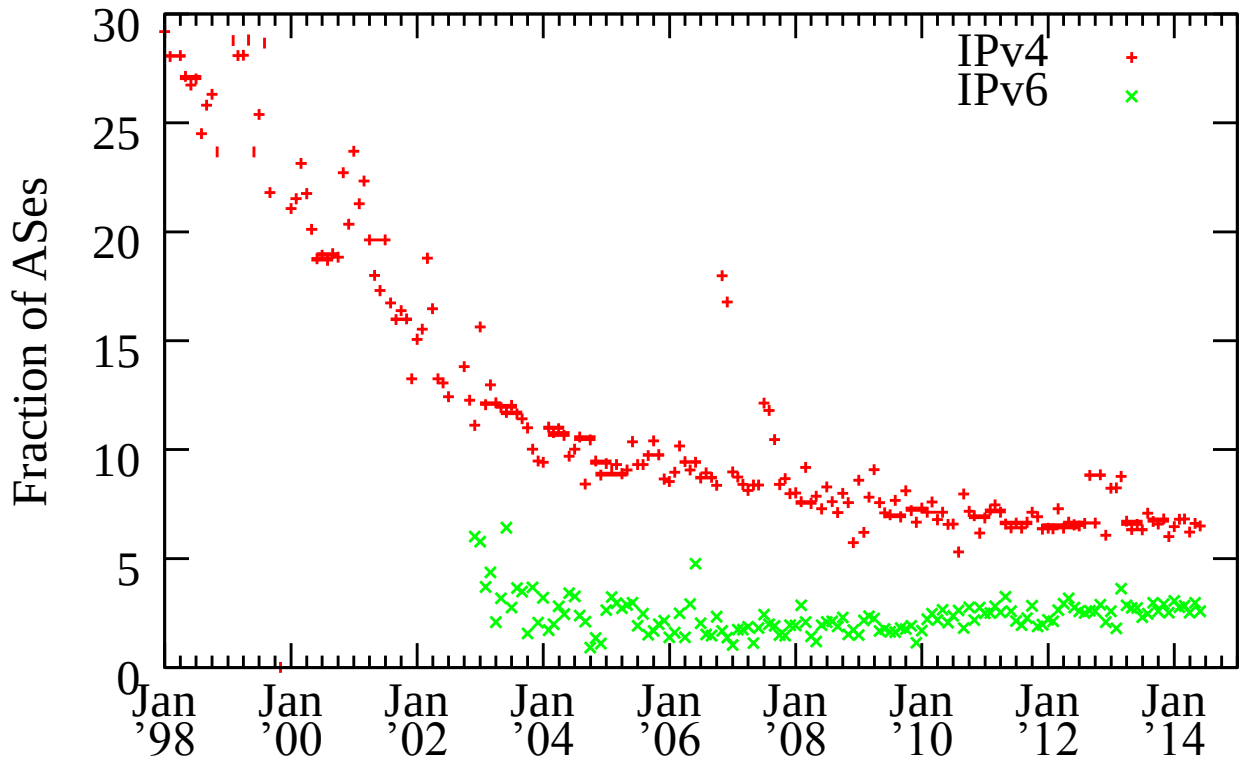
- Build traffic-based SAV analysis system
  - open-source traffic analysis system to infer evidence that ASes at an IXP have not deployed SAV best practices



- Enabling SAV testing in home networks
  - build software to operate on OpenWrt platform with weekly test as part of default configuration.

Approach: Increased BGP stability and ingress access lists

During 2014, ≈6% and ≈3% of ASes announced different IPv4 and IPv6 addresses month-to-month, respectively. Increased stability may make it feasible to use static ingress access lists.



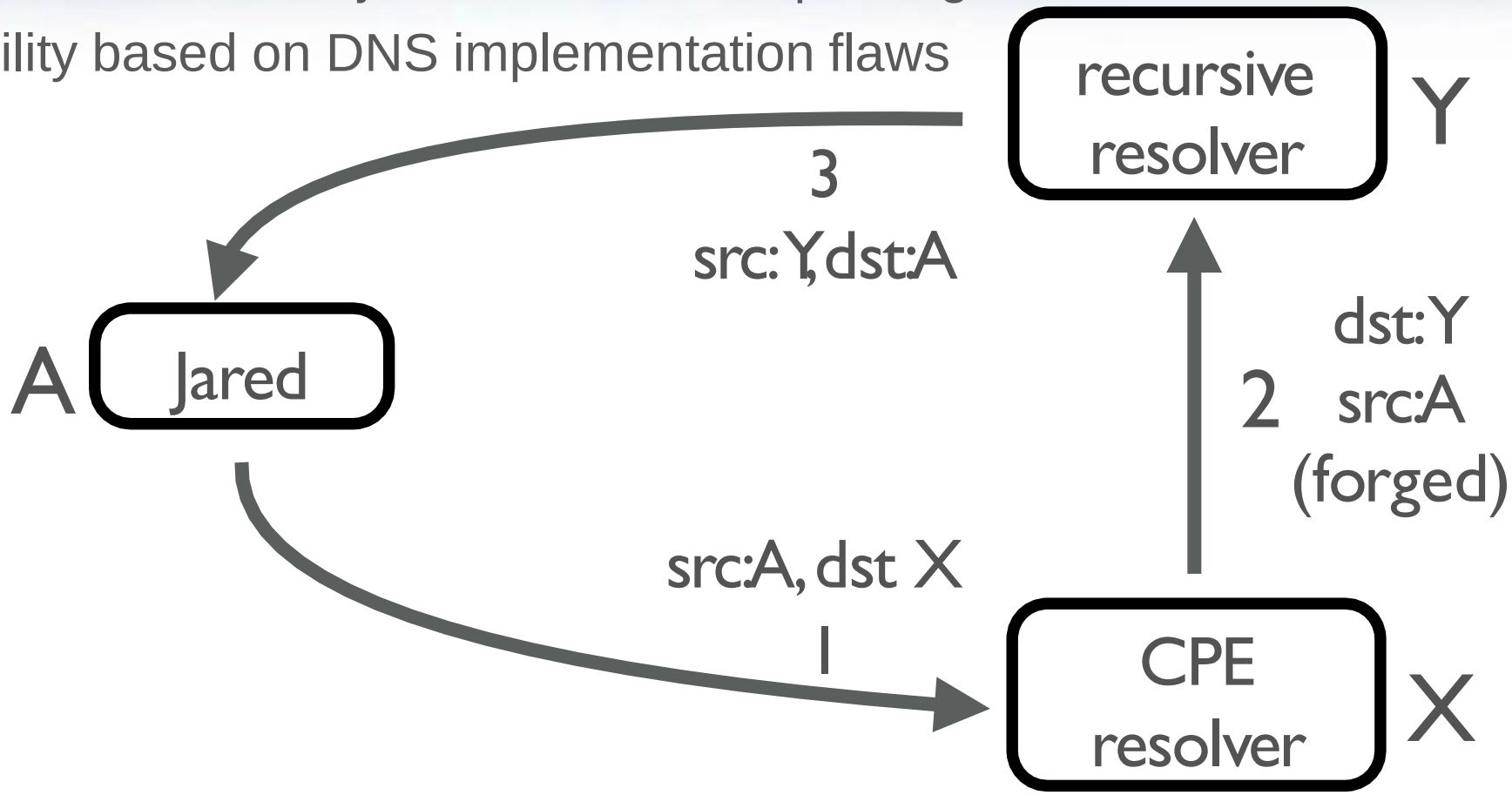
ASes whose address space announcements change month-to-month.

Benefits

- Measurement platform to test IP source address validation best practice (BCP38) compliance.
- Strategies for mitigating susceptibility to DDoS attacks that have become threat to national security, commerce, and critical infrastructure.
- Software tools will use open source licenses.
- Project targets BAA TTA #1 goal of focusing BCP38 compliance attention where it will most benefit.

~~Competition~~ – Related Work

OpenResolverProject: Detection of spoofing ability based on DNS implementation flaws



357K of 17M, as at 2 Aug 2015

Current Status: Infrastructure

Measurement Infrastructure: 119 Ark nodes

- hosting spoofing experiments as well as: TCP characteristics, DNSSEC, IPv6 evolution, outages, BGP hijacks, congestion maps

Servers: web and data server spoofer.caida.org

http://www.caida.org/projects/ark/

Current Status: Statistics (country)

Spoofer Project: Country stats (within last

Country	Client Prefixes	Spoofing Prefixes	Blocking Prefixes	Inconsistent Prefixes
usa	1748	415 (23.7%)	1297 (74.2%)	36 (2.1%)
ind	277	95 (34.3%)	178 (64.3%)	4 (1.4%)
gbr	208	54 (26.0%)	148 (71.2%)	6 (2.9%)
can	215	51 (23.7%)	162 (75.3%)	2 (0.9%)
ita	160	41 (25.6%)	113 (70.6%)	6 (3.8%)
nld	180	33 (18.3%)	138 (76.7%)	9 (5.0%)
deu	166	32 (19.3%)	131 (78.9%)	3 (1.8%)
swe	88	32 (36.4%)	55 (62.5%)	1 (1.1%)
aus	94	30 (31.9%)	63 (67.0%)	1 (1.1%)
jpn	60	28 (46.7%)	29 (48.3%)	3 (5.0%)
rus	99	28 (28.3%)	70 (70.7%)	1 (1.0%)
rou	67	24 (35.8%)	41 (61.2%)	2 (3.0%)
kor	184	23 (12.5%)	154 (83.7%)	7 (3.8%)
fra	99	22 (22.2%)	75 (75.8%)	2 (2.0%)
bra	98	21 (21.4%)	77 (78.6%)	0 (0.0%)
isr	37	20 (54.1%)	16 (43.2%)	1 (2.7%)
che	52	19 (36.5%)	30 (57.7%)	3 (5.8%)
idn	41	19 (46.3%)	22 (53.7%)	0 (0.0%)
tur	58	19 (32.8%)	38 (65.5%)	1 (1.7%)
chn	57	18 (31.6%)	38 (66.7%)	1 (1.8%)
phl	44	16 (36.4%)	28 (63.6%)	0 (0.0%)
pol	72	16 (22.2%)	55 (76.4%)	1 (1.4%)
bgr	40	13 (32.5%)	25 (62.5%)	2 (5.0%)
aut	29	12 (41.4%)	17 (58.6%)	0 (0.0%)

Current Status: Statistics by ISP

Spoofer Project: AS stats (within last year)

ASN	Client Prefixes	Spoofing Prefixes	Blocking Prefixes	Inconsistent Prefixes
36352	51	28 (54.9%)	20 (39.2%)	5 (9.8%)
24560	54	17 (31.5%)	36 (66.7%)	1 (1.9%)
3269	48	14 (29.2%)	32 (66.7%)	2 (4.2%)
8551	19	13 (68.4%)	6 (31.6%)	0 (0.0%)
174	16	12 (75.0%)	5 (31.3%)	0 (0.0%)
17917	14	12 (85.7%)	0 (0.0%)	2 (14.3%)
6830	63	10 (15.9%)	49 (77.8%)	4 (6.3%)
1267	21	10 (47.6%)	10 (47.6%)	1 (4.8%)
20473	14	9 (64.3%)	3 (21.4%)	2 (14.3%)
17488	18	9 (50.0%)	9 (50.0%)	0 (0.0%)
9829	55	9 (16.4%)	46 (83.6%)	0 (0.0%)
5769	23	8 (34.8%)	15 (65.2%)	0 (0.0%)
13768	15	8 (53.3%)	7 (46.7%)	0 (0.0%)
5089	45	8 (17.8%)	34 (75.6%)	3 (6.7%)
9299	22	8 (36.4%)	14 (63.6%)	0 (0.0%)
47331	32	8 (25.0%)	24 (75.0%)	0 (0.0%)
22773	71	8 (11.3%)	63 (88.7%)	0 (0.0%)
20115	74	8 (10.8%)	66 (89.2%)	0 (0.0%)
8452	26	7 (26.9%)	19 (73.1%)	0 (0.0%)
3356	13	7 (53.8%)	4 (30.8%)	2 (15.4%)
8151	26	7 (26.9%)	19 (73.1%)	0 (0.0%)
209	25	7 (28.0%)	18 (72.0%)	0 (0.0%)
7545	9	6 (66.7%)	3 (33.3%)	0 (0.0%)
701	93	6 (6.5%)	87 (93.5%)	0 (0.0%)
46573	6	6 (100.0%)	0 (0.0%)	0 (0.0%)
33182	9	6 (66.7%)	3 (33.3%)	0 (0.0%)

Next Steps

- Period 2
  - Client/Server software updates (May 2016)
  - System demonstration to DHS (May 2016)
  - Updated reporting system (Oct 2016)
  - Report on viability of IXP SAV system (Oct 2016)
  - Expanded SAV report new data types (Mar 2017)
  - Client/Server software updates (Mar 2017)
- Period 3
  - Updated reporting system (Aug 2017)
  - Tool to measure IXP SAV deployment (Dec 2017)
  - Report feedback from IXPs (Apr 2018)
  - Final client/server release (Jun 2018)
  - Final report (Jul 2018)

Proposal Title: Software Systems for Surveying Spoofing Susceptibility
4 August 2015

Photograph or Artist concept / Technical Approach:

Operational Capability/Benefits:

- Measurement platform to test IP source address validation best practice (BCP38) compliance.
- Strategies for mitigating susceptibility to DDoS attacks that have become threat to national security, commerce, and critical infrastructure.
- Software tools will be released with open source licenses.
- Project targets BAA TTA #1 goals of focusing BCP38 compliance attention where it will have the highest benefit.

Proposed Technical Approach:

1. We will develop new measurement tools, analysis capabilities, and data sets to enable assessment and improvement of BCP38 compliance, to minimize Internet's susceptibility to spoofed DDoS attacks.
2. Task 1: Production-quality client-server source address validation (SAV) testing system, easily deployable by enterprise networks. Task 2: Database, analysis, and reporting system to guide compliance attention where it can have most positive impact. Task 3: Traffic SAV-analysis system development to support expanded coverage of SAV testing at IXPs. Tasks 4: Home-router software modules to support compliance testing by less technical users.
3. Prototype system intermittently operational for last 5 years, informing proposed design and development.
4. We assisted Dr. Beverly with keeping current system somewhat operational without dedicated funding, We have ongoing collaborations with IXP (Task 3) and open-source home router vendor (Task 4).
5. Synergies with DHS&NSF-funded infrastructure and research projects (Internet mapping Ark platform, UCSD network-telescope), IPv6 evolution, & Internet-wide active measurement software (scamper).

Schedule, Milestones,Deliverables & Contact Info

- Milestones:. Project starts 1 Aug 2015. Initial release of replacement client-server software: by 1 May 2016, subsequent releases every 6 mo. Reporting system to inform operational and policy stakeholders: 1 May 2016; updates every 6 mo. Report on feasibility of IXP traffic SAV-analysis system: 1 Oct 2016. Development of IXP traffic SAV system: 1 Dec 2017. Development of home router software: 1 Apr 2018.
- Project duration: Total period of performance: 1 Aug 2015 - 31 Jul 2018 (36 months).
- Deliverables: quarterly reports, tool releases, reporting system, annual reports with updates to technical approach.
- POC: Shelby Mayoral, UCSD Contracts&Grants, 9500 Gilman Dr. MC 0934, La Jolla, CA 92093-0934 FAX 858-534-0280.