DHS S&T

CYBER SECURITY DIVISION – Program Manager – Daniel Massey

DDoSD Kickoff Meeting, CSU Fort Collins, CO

TTA 1: Software Systems for Surveying Spoofing Susceptibility

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

Team Profile

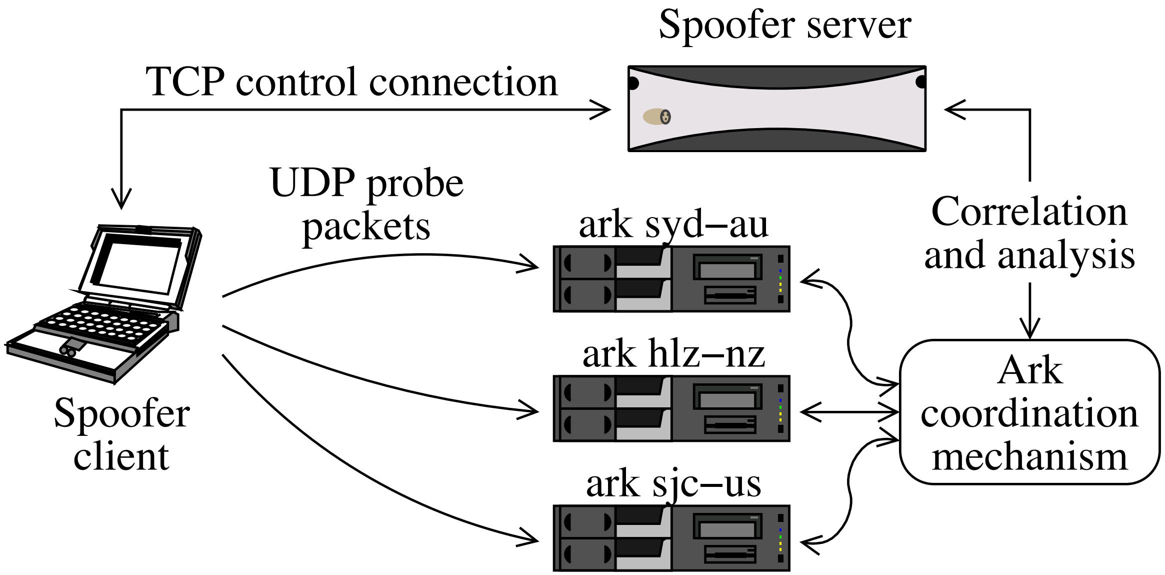
The Center for Applied Internet Data Analysis (CAIDA)

- – 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

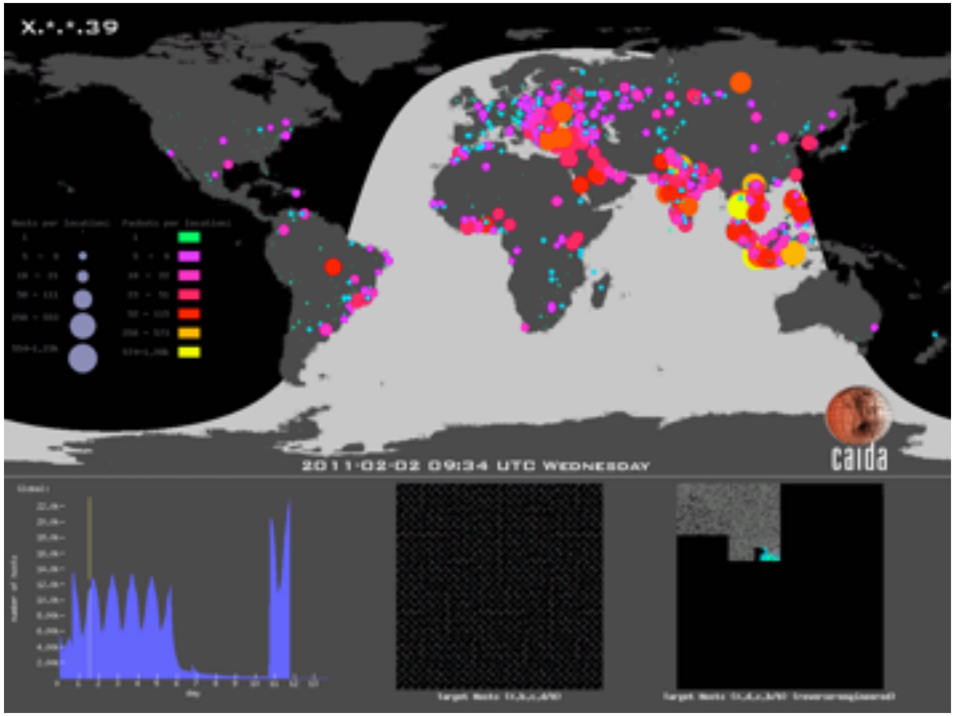
Develop, test and deploy new tools to measure and report on the deployment of source address validation (SAV) best practices.



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

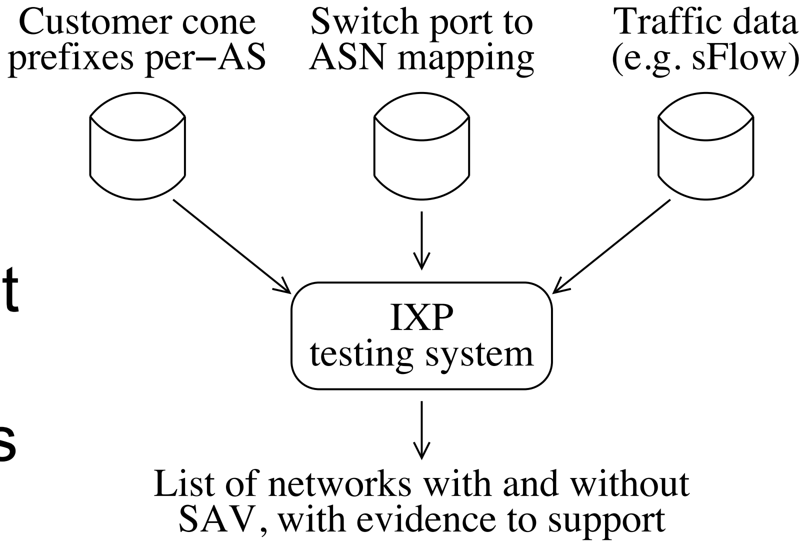
Approach

- **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

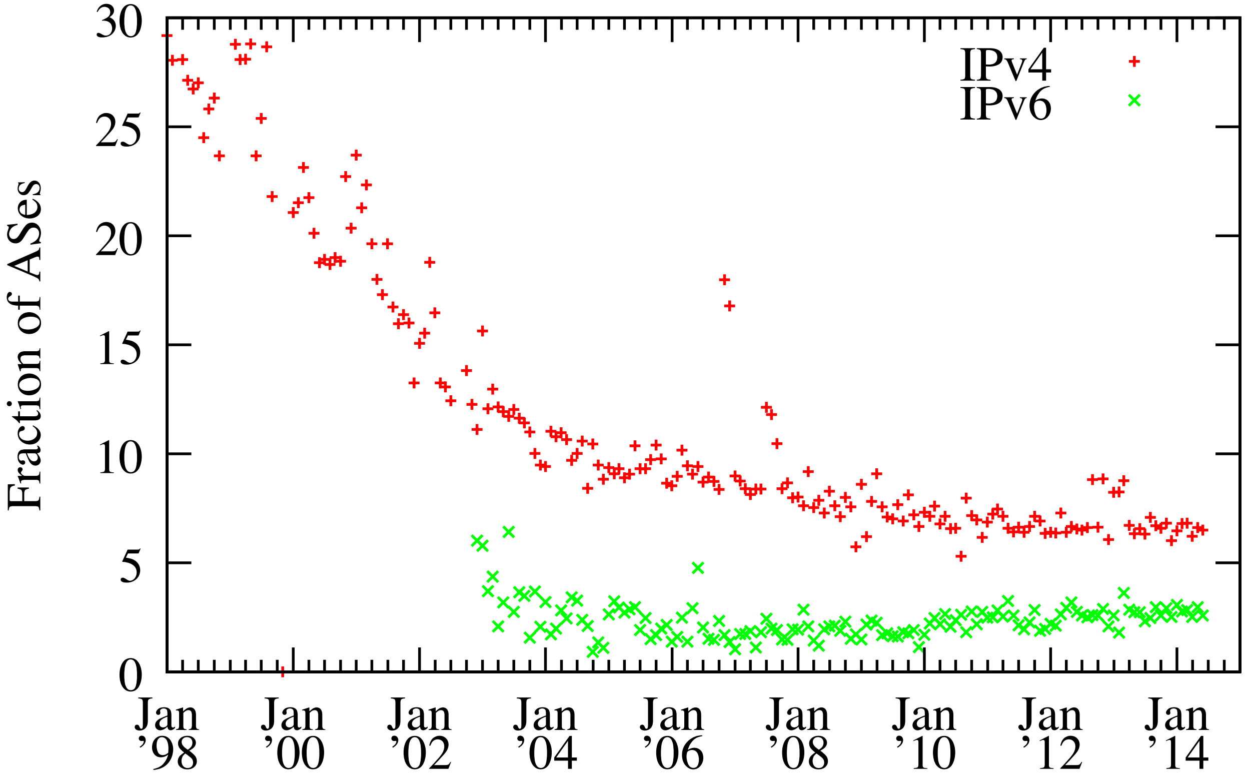
Approach

- **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


Customer cone prefixes per−AS
Switch port to ASN mapping
Traffic data (e.g. sFlow)
IXP testing system
List of networks with and without SAV, with evidence to support

- **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 static ingress access lists



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

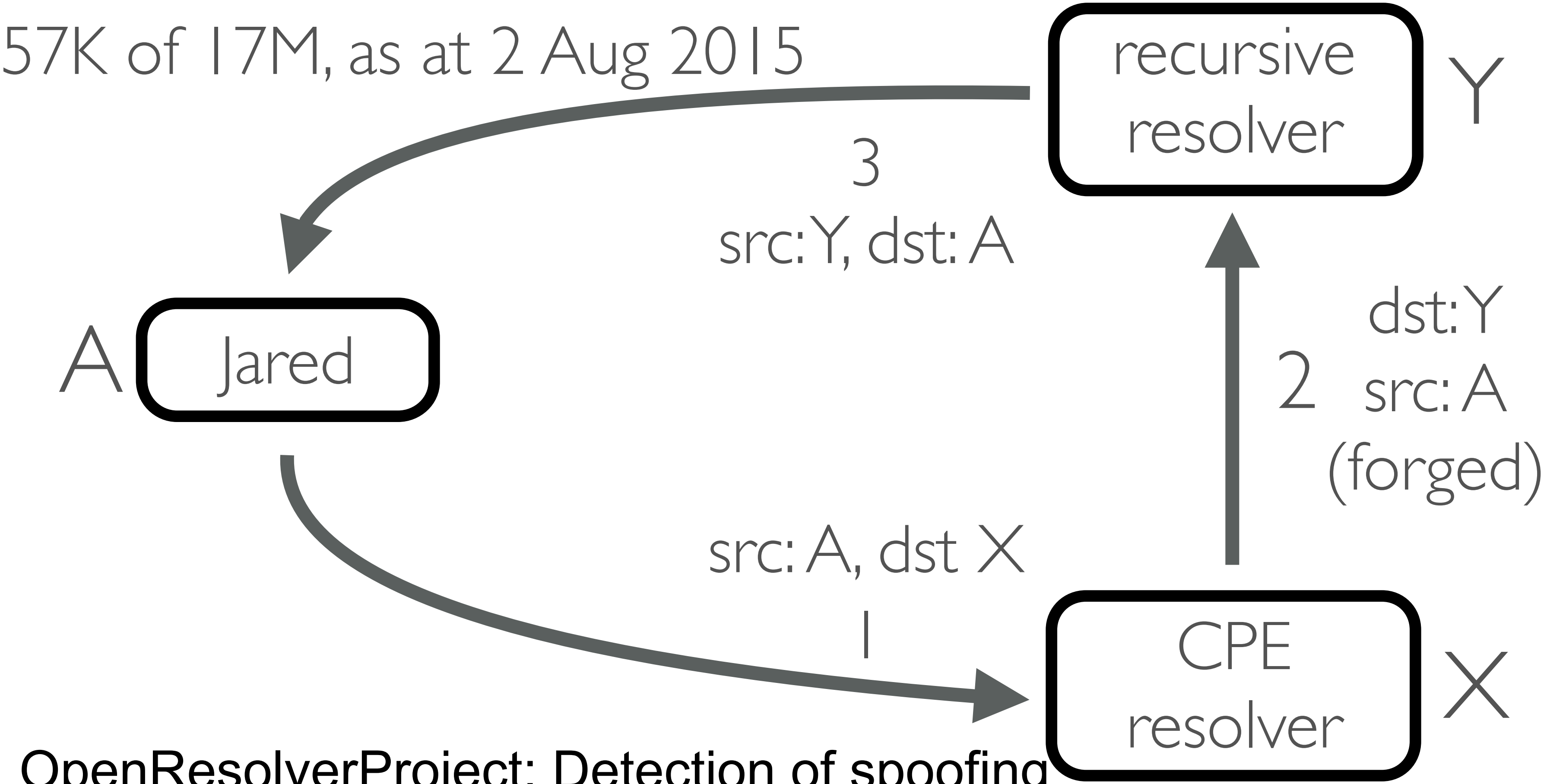
During 2014, ≈6% and ≈3% of ASes announced different IPv4 and IPv6 addresses month-to-month, respectively. Increased stability may make it feasible to use static ingress access lists.

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

357K of 17M, as at 2 Aug 2015



recursive resolver

Y

3
src: Y, dst: A

A

Jared

dst: Y
2 src: A
(forged)

src: A, dst X
1

CPE resolver

X

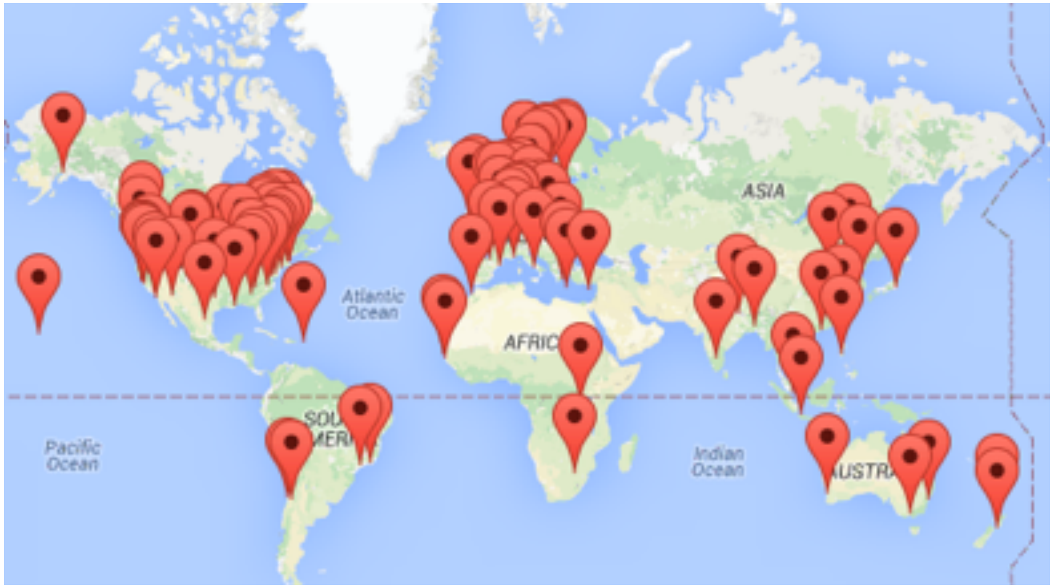
OpenResolverProject: Detection of spoofing ability based on DNS implementation flaws

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

- **Milestones**
  - Initial release of software: May 2016; releases every 6 mo.
  - reporting system: May 2016; releases every 6 mo.
  - Report on feasibility of IXP traffic SAV-analysis system: Oct 2016
  - Development of IXP traffic SAV system: Dec 2017
  - Development of home router software: Apr 2018
- **Schedule**
  - Project duration 1 August 2015 - July 2018 (36 months)
    - Period 1: Applied Research and Development (8 months)
    - Period 2: Development (12 months)
    - Period 3: Development and Tech Demo (16 months)
- **Deliverables**
  - Quarterly reports, tool releases, reporting system, annual reports with updates to technical approach.

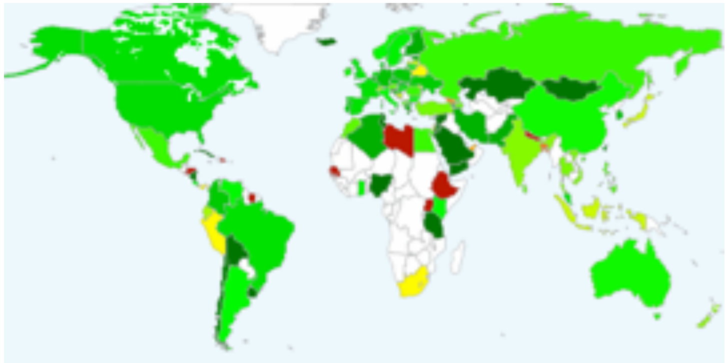
Next Steps

- 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)

Project Quad Chart

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.