Recent Results in Network Mapping: Implications on Cybersecurity

Robert Beverly, Justin Rohrer, Geoffrey Xie

Naval Postgraduate School
Center for Measurement and Analysis of Network Data (CMAND)

July 27, 2015

DHS S&T Cyber Seminar

cMAND

Outline

cMAND

CMAND Lab @ NPS

Naval Postgraduate School

- Navy's Research University
- Located in Monterey, CA
- $\simeq$1500 students, military officers, foreign military, DoD civilians

Center for Measurement and Analysis of Network Data

- 3 NPS professors, 2 NPS staff
- 1 PhD student, rotating cast of $\sim$ 5-8 Master's students
- Collaborators: CAIDA, ICSI, MIT, Akamai, Cisco, Verisign, ...

Focus:

- Large-scale network measurement and data mining
- Network architecture and security

Select Recent Publications (**bold** DHS-supported):

1. Luckie, Beverly, Wu, Allman, Claffy, "*Resilience of Deployed TCP to Blind Off-Path Attacks*," in ACM IMC 2015
2. Huz, Bauer, Claffy, Beverly, "*Experience in using Mechanical Turk for Network Measurement*," in ACM C2BID 2015
3. **Beverly, Luckie, Mosley, Claffy, "*Measuring and Characterizing IPv6 Router Availability*," in PAM 2015**
4. **Beverly, Berger, "*Server Siblings: Identifying Shared IPv4/IPv6 Infrastructure*," in PAM 2015**
5. **Alt, Beverly, Dainotti, "*Uncovering Network Tarpits with Degreaser*," in ACSAC 2014**
6. Craven, Beverly, Allman, "*A Middlebox-Cooperative TCP for a non End-to-End Internet*," in ACM SIGCOMM 2014
7. **Baltra, Beverly, Xie, "*Ingress Point Spreading: A New Primitive for Adaptive Active Network Mapping*," in PAM 2014**

Outline

cMAND

Network Measurement

Network measurement is **fundamental** to cybersecurity

Passive Measurement

- Listen (promiscuously) to traffic
- Gain understanding of Tactics, Techniques and Procedures:
  - Type of attacks and methods
  - Dispersion (sources and targets)
  - Prevalence and intensity
- Detect emergent threats:
  - New attacks and attack vectors
- Invaluable intelligence for cyber operations and research

Network Measurement

Active measurement:

- Send specially tailored probes to targeted destinations
- Elicit particular behaviors, make stronger inferences
- Examples of active measurements:
  - Internet-wide vulnerability scanning (e.g., heartbleed, blind TCP attacks)
  - Topology mapping (e.g., interconnection of network service providers)
  - Fingerprinting (e.g., finding physical router w/ multiple interfaces)
  - Network hygiene (e.g., Spoofer project to measure ingress filtering – **DHS funded transition** to CAIDA for production support)

cMAND

Network Measurement

Challenges (or, why network measurement is research)

- Internet (and TCP/IP protocol suite) not designed to be measured
  - Many tools and techniques are “Tricks and Hacks”
  - Service providers don’t want to be measured (competitive, economic reasons)
  - Best common security practices often prevent measurement
- Millions or billions of measurements often required
- Dependence on location and quantity of vantage points
- Lots of large data (packets, flows, routing messages, topology, etc)
- $\rightarrow$ Needle in haystack: data mining

cMAND

Network Measurement

Even more difficult in cyber domain:

- Attacks may be targeted, difficult to observe
- No integrity or authentication of responses when probing network
- Abuse and attacks often employ obfuscation and anonymity
- $\rightarrow$ measurement results depend on fragile inferences

Outline

cMAND

Project Overview

High-Frequency Active Internet Topology Mapping:

- DHS S&T BAA-11-02 Cyber Security Division
- TTA #7 “Network Mapping and Measurement”
- Q4 2012 – Q3 2015

Project Objective

Goal:

- Develop new techniques that improve state-of-the-art in network mapping.

Specifically:

- Obtain accurate network graphs, at interface and router granularities, even at large scale (i.e. Internet) and amid topological sparsity (e.g. IPv6) and obfuscation.
- Obtain topologies faster than existing systems to better capture transient dynamics, including malicious or misconfiguration events.
- Working systems implementation, with transfer to production mapping systems.

Motivation (from DHS BAA):

"The protection of cyber infrastructure depends on the ability to identify critical Internet resources, incorporating an understanding of geographic and topological mapping of Internet hosts and routers. A better understanding of connectivity richness among ISPs will help to identify critical infrastructure. Associated data analysis will allow better understanding of peering relationships, and will help identify infrastructure components in greatest need of protection. Improved router level maps (both logical and physical) will enhance Internet monitoring and modeling capabilities to identify threats and predict the cascading impacts of various damage scenarios."

These proposed capabilities are critical to U.S. national security missions, analyses of cyber infrastructure threats and risks, and hardening of U.S. military, as well as civilian, Internet communications environments.

Network Mapping – Motivation:

- Protect and improve critical infrastructure
- Understand structural properties of the Internet topology, including robustness, vulnerability to attack, potential for correlated failures, IPv4/IPv6 interdependence, etc.
- Enabler of other work
  - Understanding peering/interconnection (how will traffic flow if X happens?)
  - Data vs. control plane correlation (is there a route hijack?)
  - Content Distribution optimization (where is nearest/fastest cache?)
  - IP geolocation (where is a host physically located?)
  - Reverse traceroute (what path does data take in reverse?)
  - Evolution/longitudinal studies (competition/economics, robustness)
  - . . .

Outline

cMAND

ACSAC 2014

“Uncovering Network Tarpits with Degreaser”
Alt et al. ACSAC 2014

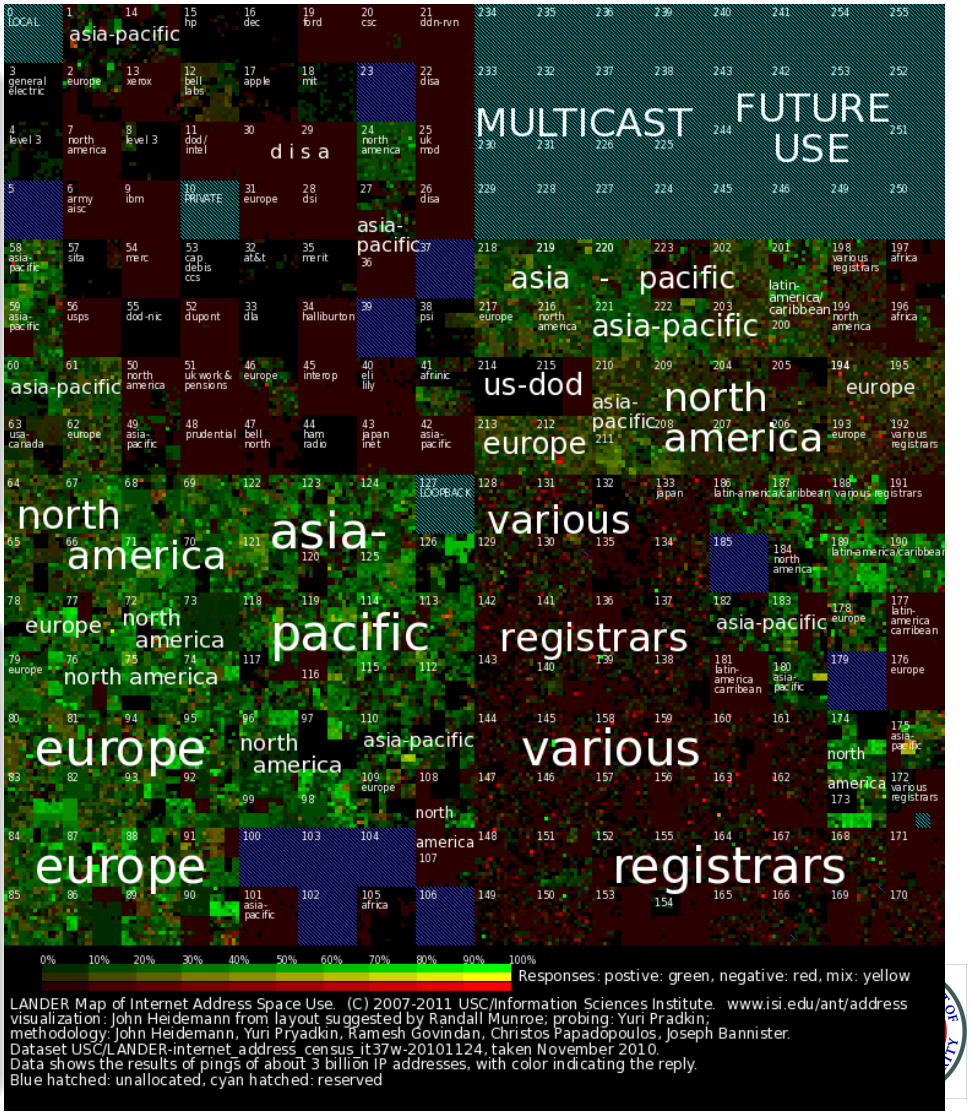
Active Cyber Defense

- Typical assumption for active network measurements: a host either responds (truthfully) to a probe or does not respond at all
- For instance, a non-response:
  - Firewall or other blocking
  - Protocol/service/measurement trick not supported
- Alternate choice: deception
  - Provide a false response to influence adversary's behavior
  - Canonical example: honeypots
- We're interested in: fake networks, fake hosts, fake paths

Motivation

- How prevalent are deceptive networks/hosts on the Internet?
- How do Internet topology and census scans treat these "fake" networks?

- ACSAC 2014: finding network tarpits
- Synergistic w/ DHS sponsored census work (John Heidemann @ USC/ISI)
- **Is this real??** $\Rightarrow$



The Target: Tarpits

Network Tarpits

- Attempt to slow (or stop) various forms of network scanning
- General Idea:
  - A single machine pretends to be all unused hosts on a subnetwork
  - Answers for all requests to those fake hosts
  - Holds the TCP connection by setting TCP window to zero...
  - And never letting go ...
- Two well-known applications:
  - LaBrea
  - Linux Netfilter (TARPIT/DELUDE plugins)

cMAND

LaBrea

LaBrea TCP Response

- After layer-2 capture, LaBrea responds to ICMP and any TCP port
- SYN/ACK has an advertised window of 10 (or 3), and no TCP options
- This window flow-controls connection, but keeps it active (consuming remote scanner's resources)
- Example HTTP from `10.1.10.102` to `10.1.10.210`:

```
06:20:47.971276 IP 10.1.10.102.51161 > 10.1.10.210.http: Flags [S], seq 3536100821, win 65535,
            options [mss 1460,nop,wscale 4,nop,nop,TS val 1194569089 ecr 0,sackOK,eol], length
06:20:47.971475 IP 10.1.10.210.http > 10.1.10.102.51161: Flags [S.], seq 1457023515, ack 353610082
            win 10, length 0
```

LaBrea

LaBrea TCP Response

- After layer-2 capture, LaBrea responds to ICMP and any TCP port
- SYN/ACK has an advertised window of 10 (or 3), and no TCP options
- This window flow-controls connection, but keeps it active (consuming remote scanner's resources)
- Example HTTP from `10.1.10.102` to `10.1.10.210`:

```
06:20:47.971276 IP 10.1.10.102.51161 > 10.1.10.210.http: Flags [S], seq 3536100821, win 65535,
                options [mss 1460,nop,wscale 4,nop,nop,TS val 1194569089 ecr 0,sackOK,eol], length
06:20:47.971475 IP 10.1.10.210.http > 10.1.10.102.51161: Flags [S.], seq 1457023515, ack 353610082
                win 10, length 0
```

Finding Tarpits

Simple Techniques Do Not Work:

- Subnet occupancy: high-occupancy subnets are often content caches and hosting providers
- Response time: unreliable due to ARP caching and hard capture
- Hosts listening on all ports: search space too large, doesn't find single-port tarpits

Introducing Degreaser

New tool: *Degreaser*

- Network scanner to find tarpits
- Multi-threaded, C++
- Open Source (currently on github)
- Can detect:
  - LaBrea Persistent (LaBrea-P)
  - LaBrea Non-persistent (LaBrea-NP)
  - Netfilter TARPIT (iptables-T)
  - Netfilter DELUDE (iptables-D)

Introducing Degreaser

Degreaser: Network scanner to find tarpits

```
IP:    311552/496690176   Scanned IPs: 311552          Excluded IPs: 0
Real Hosts: 0             Rejecting Hosts: 5062        Errors: 15225
Tarpits: 125335           LaBrea: 123739               iptables(tarpit): 1596
                                                       iptables(delude): 9414
  1% [==>                                                                  ]
IP Address            Response Time    Window Size  TCP Flags   TCP Options  Scan Result
199.133.85.176             95885           0                                 Error in TCP packet
136.227.165.15            165304           0       SA           M           LaBrea
148.228.33.42                  0           0                                 No response
209.129.242.227                0           0                                 No response
188.118.162.36            222828           0                                 Unreachable
208.184.85.68                  0           0                                 No response
108.59.196.198            106382           0       SA           M           LaBrea
203.106.97.168                 0           0                                 No response
210.240.212.93            181553           0       SA           M           LaBrea
196.74.235.92                  0           0                                 No response
197.61.159.19                  0           0                                 No response
195.232.132.215                0           0                                 No response
202.38.248.236                 0           0                                 No response
```

Degreaser

Degreaser Internals

- Sends TCP SYN to host and waits for responding SYN/ACK
- Window size. Is it abnormally small?
- What TCP options, if any, are returned?
- But Wait:
  - A real host might legitimately have a small window size and not use options.

cMAND

Detection Algorithm

Tease apart real vs. fake hosts:

Send a data packet of size one less than the window size

- A real host would send an ACK; neither LaBrea nor Netfilter do!
- Data packet can distinguish between LaBrea and Netfilter:
  - LaBrea: Won't respond with ACK unless payload $>$ window size
  - Netfilter: Immediately sets window to zero.

Distinguishing between LaBrea-P and LaBrea-NP:

- Send a zero-window probe
  - LaBrea-P: Responds with zero-win ACK
  - LaBrea-NP: No response

Special Case: Zero Window

- Can't send a data packet, so we send a FIN
- Response? $\rightarrow$ real host, else: other

Detection in the Wild

Googling

- Does anyone actually admit to using this stuff?
  - We found only one company (3 tarpitting IP addresses)

Instead:

- Scanned at least one host in all routed /24 subnets (over 20 million IP addresses)
- Used cryptographic permutation to randomize the scan: avoid triggering IDS/anomaly detectors
- Found **1,451** tarpitting IPs directly via *degreaser*
- Exhaustive scan on subnets containing these hosts

Detection in the Wild

Googling

- Does anyone actually admit to using this stuff?
  - We found only one company (3 tarpitting IP addresses)

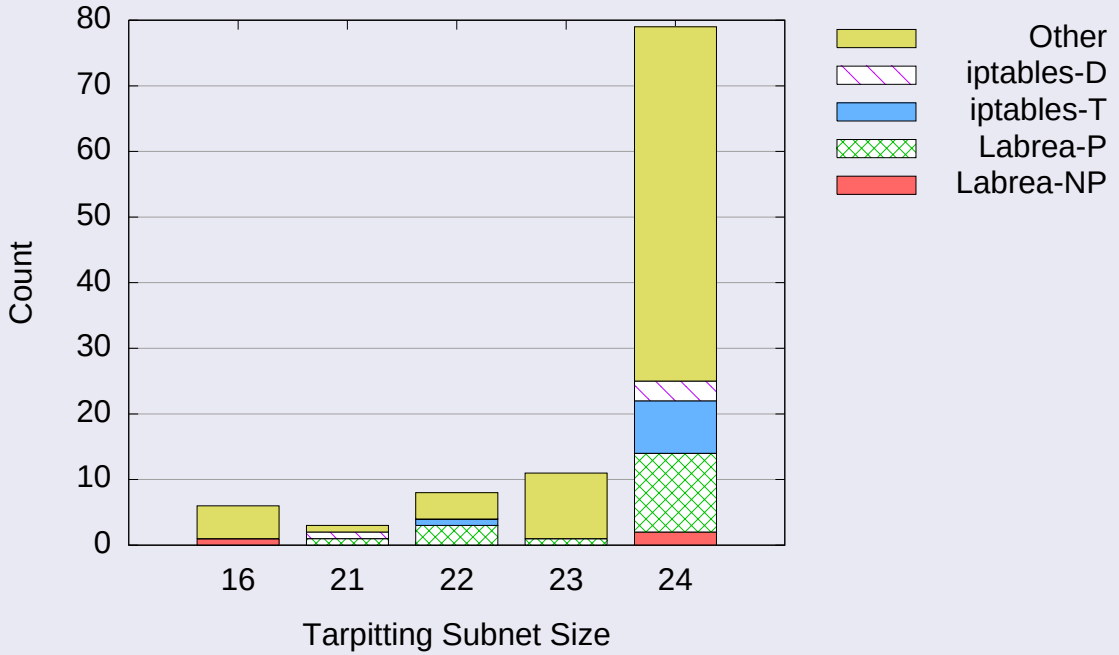
Instead:

- Scanned at least one host in all routed /24 subnets (over 20 million IP addresses)
- Used cryptographic permutation to randomize the scan: avoid triggering IDS/anomaly detectors
- Found **1,451** tarpitting IPs directly via *degreaser*
- Exhaustive scan on subnets containing these hosts

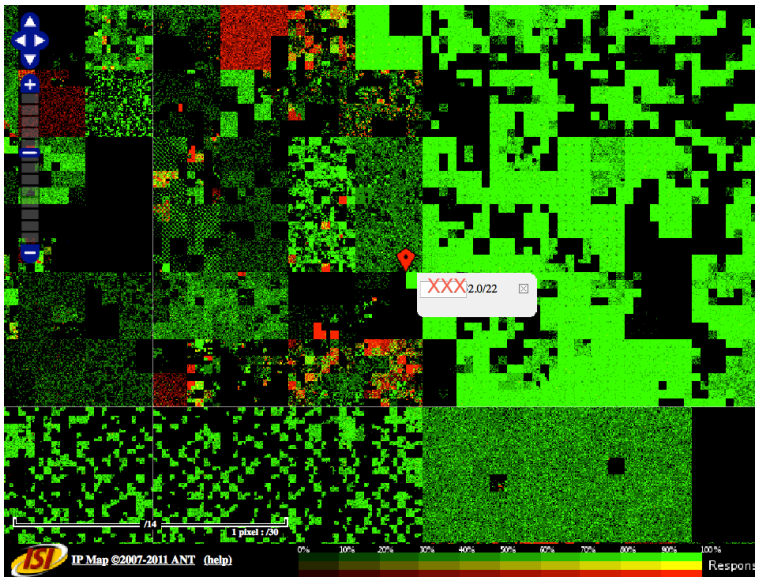
Results

Scanning Results

- Largest Subnet: Six /16!
- >**215,000** tarpit addresses
- Distributed across countries/networks
- 77 autonomous systems
- 29 countries
- Obtained validation from one provider



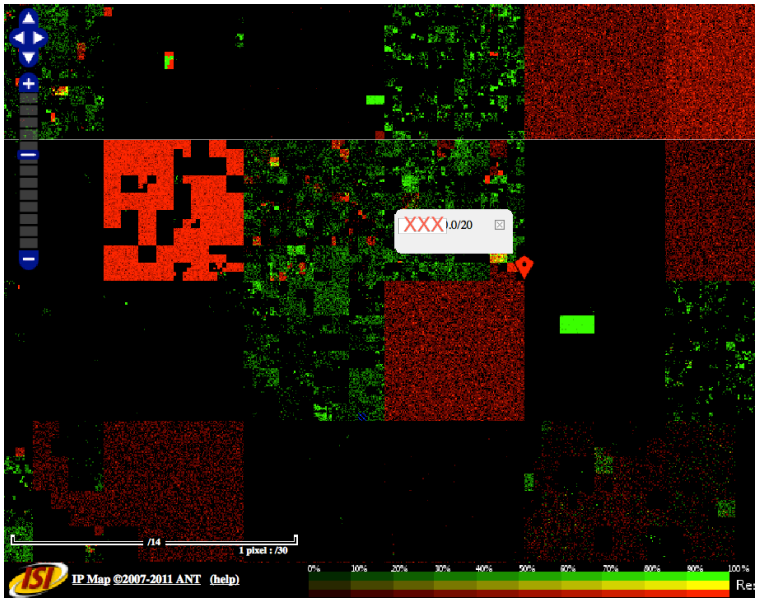
Results

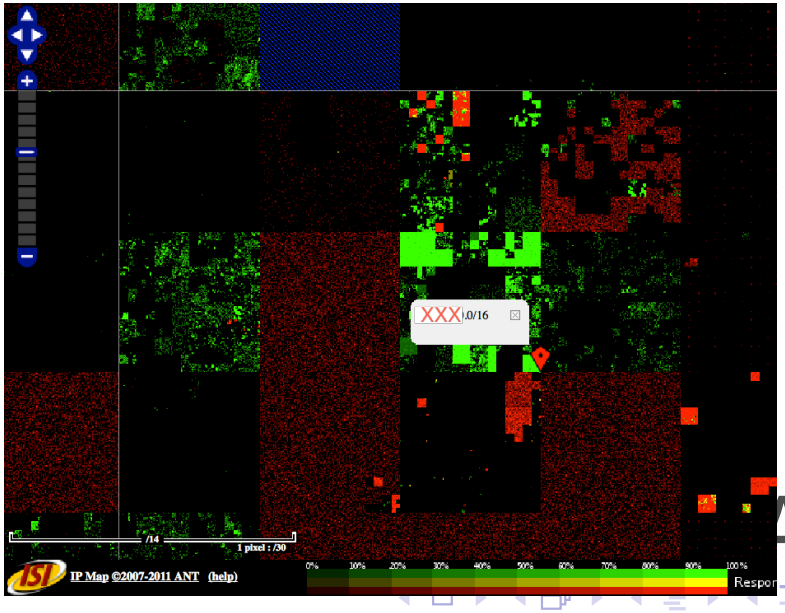


Examples from the ISI Internet Census Data:

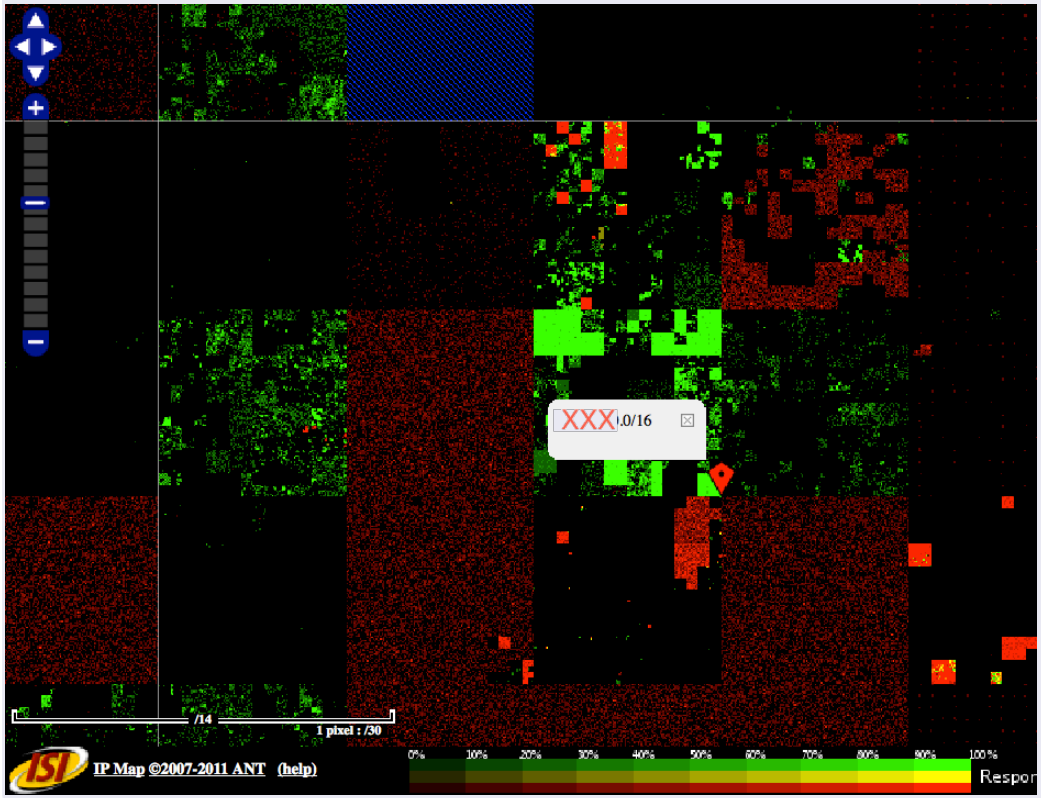
Are the indicated blocks of green cells high occupancy subnets?

Nope. All fake.





ISI Internet Census Data



For example, this /16:

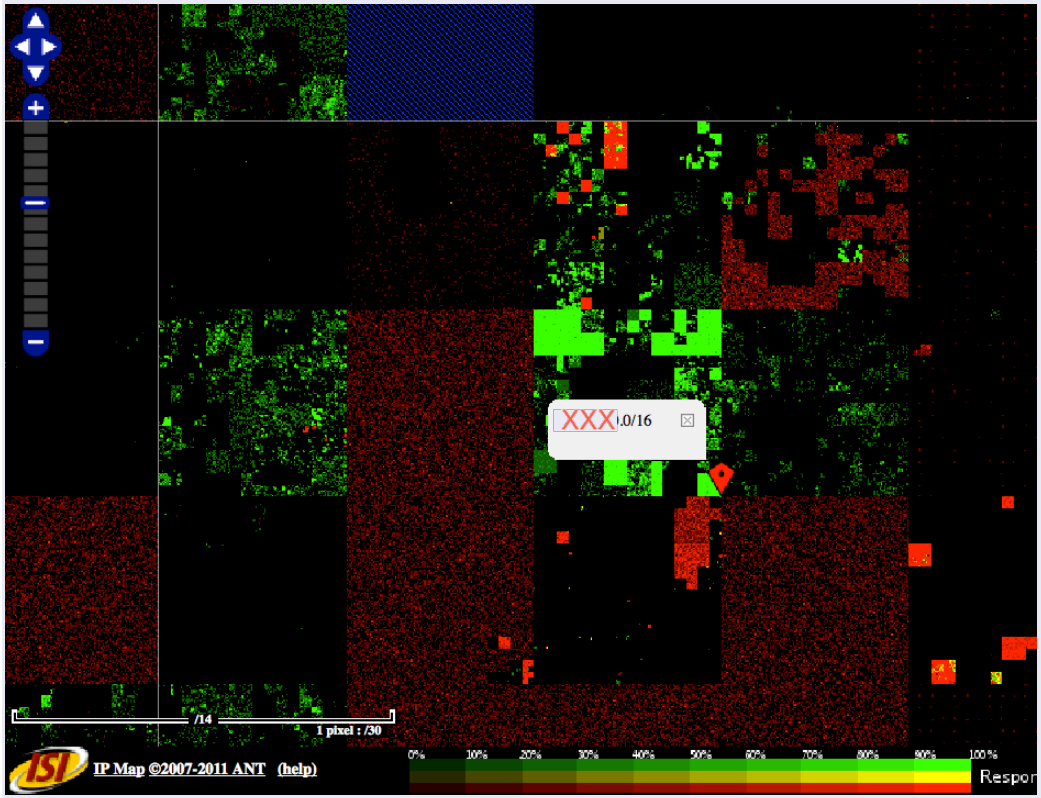
- 58 (of 256 possible) /24 subnetworks are fake (23%)

Overall:

- 2 of 6 /16's with tarpits we found are fully occupied
- These chunks represent 2^{17} fake addresses alone!

By explicitly considering deception as part of adversary's model, we can improve the robustness of our tools and measurements

ISI Internet Census Data



For example, this /16:

- 58 (of 256 possible) /24 subnetworks are fake (23%)

Overall:

- 2 of 6 /16's with tarpits we found are fully occupied
- These chunks represent 2^{17} fake addresses alone!

By explicitly considering deception as part of adversary's model, we can improve the robustness of our tools and measurements

PAM 2015

“Measuring and Characterizing IPv6 Router Availability”
Beverly et al. PAM 2015

cMAND

Infrastructure “Uptime”:

- More formally: uninterrupted system availability
- Duration between device restarts
- Restarts due e.g. to planned device reboots, crashes, power failures

cMAND

Why

Who wants uptime data?

- Researchers
- Operators
- Policy makers
- Regulators:
  - For instance, FCC mandates reporting voice network outages (but not broadband network services)

- Despite importance of Internet as critical infrastructure, little quantitative data on Internet device availability exists!

Uptime and Security

Security Implications

- Rule out the possibility that a reboot-based security update/patch has been applied to a particular device (otherwise device likely still vulnerable)
- Determine if an attack designed to reboot a device is successful
- Gain knowledge of a network's operational practices and maintenance windows

Obtaining Remote Uptime

How to remotely obtain uptime?

- Just login?
- Management protocols (e.g. SNMP)?
  - ...requires access privilege
- Existing uptime fingerprinting tools (e.g., nmap) do not work on modern operating systems...
- And especially do not work on routers that do not accept TCP connections

cMAND

Objective

Instead, our objective:

- Find uptime of remote routers...
- which don't accept TCP connections from untrusted sources...
- without privileged access...
- using active measurement

This work is the first to directly attempt to quantify Internet-wide router network infrastructure reliability = fun!

cMAND

Obtaining an Identifier

Obtaining an Identifier for IPv6 Routers

- We leverage our prior work on IPv6 alias resolution: **too-big-trick** (PAM 2013), **speedtrap** (IMC 2013)
- To remotely obtain an identifier without privileged access
- ... that resets on reboot for most IPv6 stacks
- ... including the control-plane IPv6 stack on routers!
- Identifier: IPv6 fragment extension header ID
- (see paper for details)

Why IPv6?

- Identifier in IPv6 is large (32bits) and only increments when we probe it
- (our current work is on analogous inference w/ IPv4)

Methodology

High-Level:

- Periodically probe IPv6 routers with PTB and ICMP6 echo request (using scamper packet prober)

Real example, 3 probes per cycle:

Mar 4 21:30:01: `0x00000001, 0x00000002, 0x00000003`
Mar 5 04:25:05: `0x00000004, 0x00000005, 0x00000006`
...
Apr 21 09:39:12: `0x000001b0, 0x000001b1, 0x000001b2`
Apr 21 16:42:54: **`0x00000001`**`, 0x00000002, 0x00000003`

Real-world heterogeneity

Not as easy in practice:

- Different router vendors == different IPv6 stacks
- BSD-based devices (notably Juniper) return random fragment IDs
- Linux-based devices return cyclic fragment IDs
- Requires de-noising and filtering

Data Collection

Data

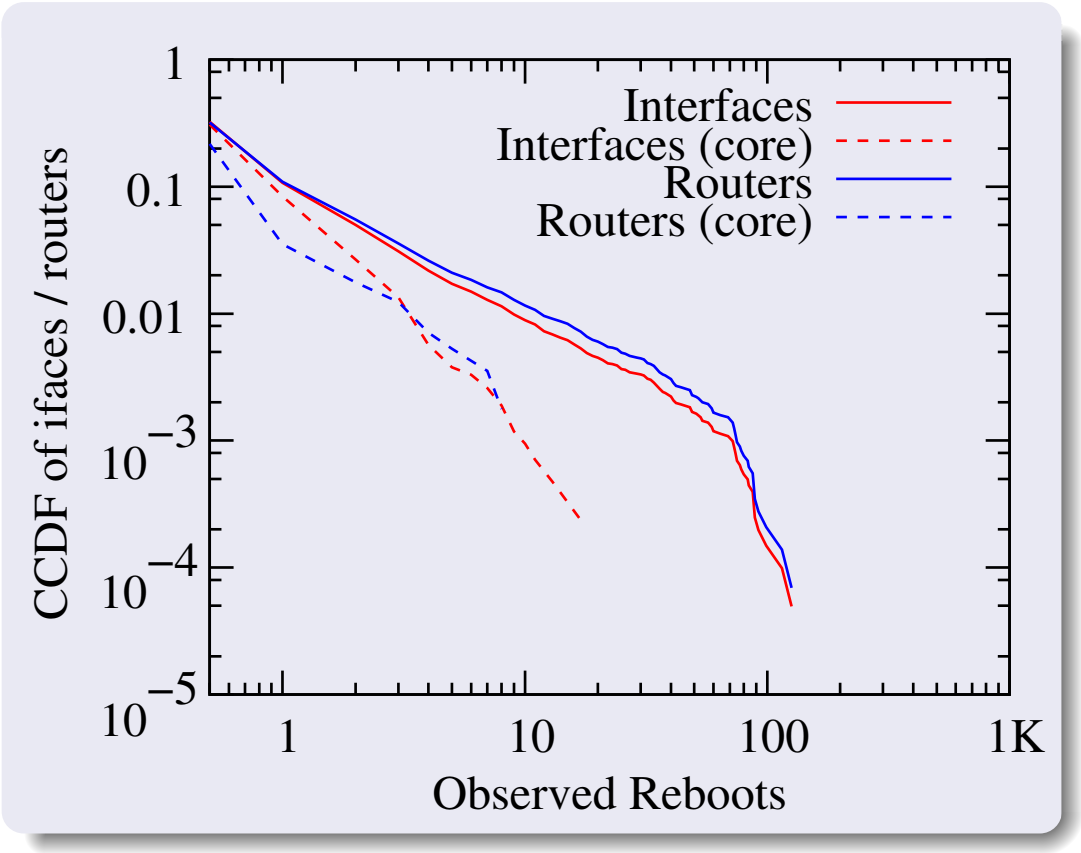
- We probed 21,539 distinct IPv6 router interfaces that return monotonic or cyclic fragment IDs
- Probed each on average every 6 hours from March 5 - July 31, 2014 from single native IPv6 vantage point

Interface Reboots → Router Reboots (see paper for details)

- Use Speedtrap to resolve aliases
- Separate into “core” routers (intra-AS) versus border routers (inter-AS)

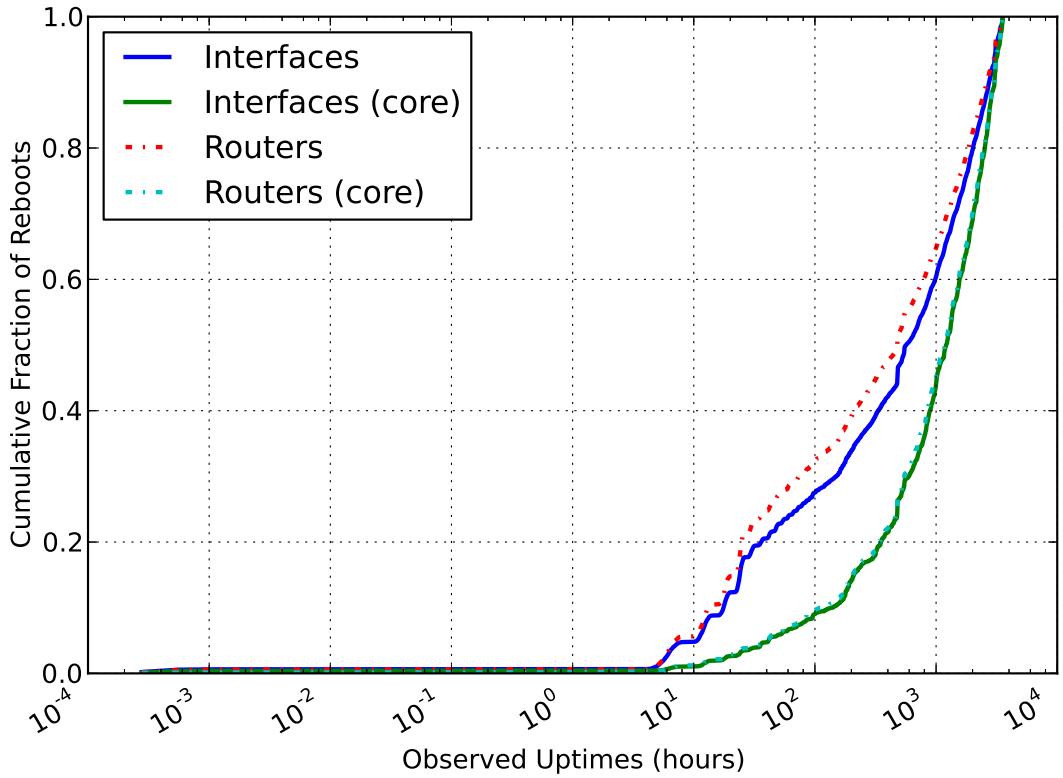
cMAND

Results



- Overall, 68% of interfaces had no reboots, while 22% had one
- Core routers and interfaces relatively more stable
- 78% of core routers had no reboots, 98% rebooted $\leq$ 2 times

Results



- Experiment duration: about 150 days
- 15% of uptimes were less than 1 day
- Median uptime of 23 days
- 10% had uptime $\geq$ 125 days

Validation

Solicited Validation from Operators of 12 ASes:

- 5 operators confirmed our inferences
- Total of 15 router restarts validated
- No false positives
- Reboots on May 18 and June 1, 2014:
  - Operators confirmed; due to TCAM exhaustion
  - Predates 512K FIB bug discussion in August, 2014!

When do Routers Reboot

- Geolocate routers to infer timezone using NetAcuity
- Weekend reboots much less likely (maintenance windows during week)

Reboots by day-of-week

	Core		All	
Monday	110	9.7%	925	11.2%
Tuesday	226	20.0%	1684	20.4%
Wednesday	227	20.0%	1553	18.8%
Thursday	197	17.4%	1313	15.9%
Friday	157	13.9%	1120	13.5%
Saturday	115	10.2%	864	10.4%
Sunday	101	8.9%	813	9.8%
	1133		8272	

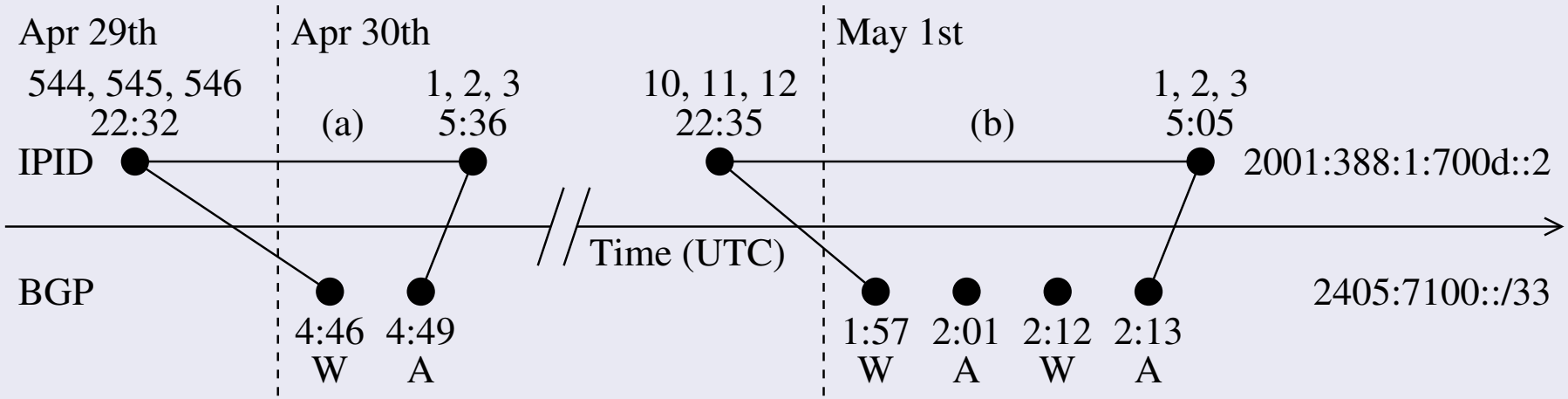
Control Plane Correlation

Correlation

- Finally, we sought to determine if the reboot events we infer are also observed in the control plane
- Focused on a customer router known to be single-homed to provider (where a globally visible withdrawal is likely when a reboot occurs)

Example Reboot Correlation w/ BGP

- Upper dots represent our inferred reboot events for router with interface `2001:388:1:700d::2`
- Lower dots represent global BGP events for the prefix (`2405:7100::/33`) announced by the router



Topology Mapping and Uptime

Correlation with BGP routing updates suggests a powerful new way to think about network resilience

- Within a densely connected ISP core with lots of redundancy, a router reboot may have no external impact
- Routers that induce globally visible routing changes are suggestive of those *most important* to the affected network prefixes

Current Work

- Investigating IPv4 uptime
- Order of magnitudes more routers, reboots, and BGP updates
- Approximately 88 IPv4 BGP events/sec from routeviews ($\sim 2.8 Bupdates/year$)
- Correlation using Apache Cassandra cluster

Topology Mapping and Uptime

Correlation with BGP routing updates suggests a powerful new way to think about network resilience

- Within a densely connected ISP core with lots of redundancy, a router reboot may have no external impact
- Routers that induce globally visible routing changes are suggestive of those *most important* to the affected network prefixes

Current Work

- Investigating IPv4 uptime
- Order of magnitudes more routers, reboots, and BGP updates
- Approximately 88 IPv4 BGP events/sec from routeviews ($\sim 2.8 Bupdates/year$)
- Correlation using Apache Cassandra cluster

Outline

cMAND

DHS Project Deliverables

- Advanced topology probing primitives; tech transfer to CAIDA and the Archipelago measurement platform (see PI meeting slides, and Baltra et al.)
- Development of “ArkQueue,” a library for more easily and efficiently interfacing with CAIDA’s Ark platform (on github)
- New probing techniques, including degreaser and uptime (code publicly available)
- Peer-reviewed academic research papers
- Tight collaboration and coordination with other DHS initiatives (CAIDA and ISI mapping work)

Our DHS funding has been spent, but the project lives on...

Follow-on collaboration with Laboratory for Telecommunication Science (LTS)

- Understanding the resilience of existing measurement tools to a deceitful adversary
- Developing an advanced tarpit based on findings from degreaser
- Investigating other sources of deceptive responses to active measurement probes, especially ability to detect fake responses to traceroute

Masters students engaged in:

- Large-scale topology emulation
- IPv6 mapping techniques (work under submission)
- Uptime measurement of other critical infrastructure, including IPv4 routers, DNS servers, web servers
- IPv4 uptime correlation and understanding most important infrastructure

Summary

- Network measurement fundamental to cybersecurity operations and research
- Active network mapping critical to understanding resilience of critical infrastructure
- Demonstrated the need to assume a deceitful adversary, and to improve the resilience of mapping tools
- Developed first technique to remotely infer the uptime of infrastructure devices without privileged access.

Thanks!

Questions?

https://www.cmand.org

cMAND