Don’t Forget to Lock the Back Door!
A Characterization of IPv6 Network Security Policy

Jakub (Jake) Czyz, University of Michigan & QuadMetrics, Inc.
Matthew Luckie, University of Waikato
Mark Allman, International Computer Science Institute
Michael Bailey, University of Illinois at Urbana-Champaign

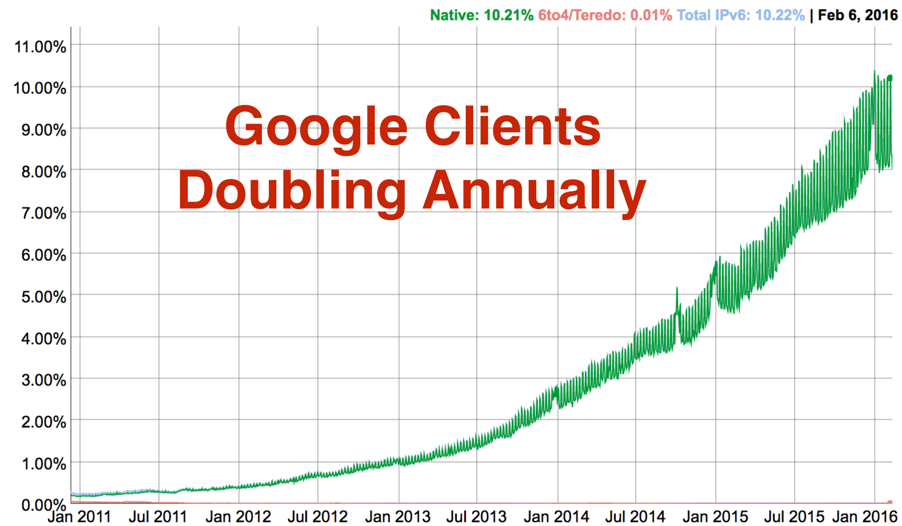
Network and Distributed System Security Symposium

2016-02-22

San Diego, CA, USA

IPv6?? Yawn… amiright?

- Actually, IPv6 adoption is now very robust. E.g.:
  - Google : 8-10%; (U.S.: 23%)
  - Facebook : 10%; (U.S.: 23%)
  - Comcast 39%. ATT 52%. Deutsch Telekom 28%



https://www.google.com/intl/en/ipv6/statistics.html

- BUT: Lack of maturity in stacks, processes, tools, operator competency

- Plus, some big misconceptions about IPv6 abound :(
  - Myth #1: IPv6 is "More Secure."

Recent operator training seminar ad:

Motivation

“ In new IPv6 deployments it has been common to see IPv6 traffic enabled but none of the typical access control mechanisms enabled for IPv6 device access. “

— IETF Draft: Operational Security Considerations for IPv6 Networks; Chittimaneni, et al., 2015; http://tools.ietf.org/html/draft-ietf-opsec-v6-07

Talk Roadmap

- Motivation
- Methodology
- Results
- Validation
- Scanning Feasibility
- Implications & Summary

Methodology: Target Lists

- **Population** of interest: global dual-stacked routers and servers
  - **Routers**: IPs from CAIDA Ark trace route dataset
  - **Servers**: from DNS ANY record queries against IPs and names discovered by Rapid7 service scanning
- **Grouping** to find all dual-stack hosts:
  - Extract hostnames with A, AAAA, and PTR records
  - Closed-set merge all dual-stack hosts linked by the same address or hostname record; finally: validate app-layer fingerprints
- End up with, ping-responsive: **25K routers; 520K servers**
  - **58% of globally-routed dual-stacked ASes; 133 countries**

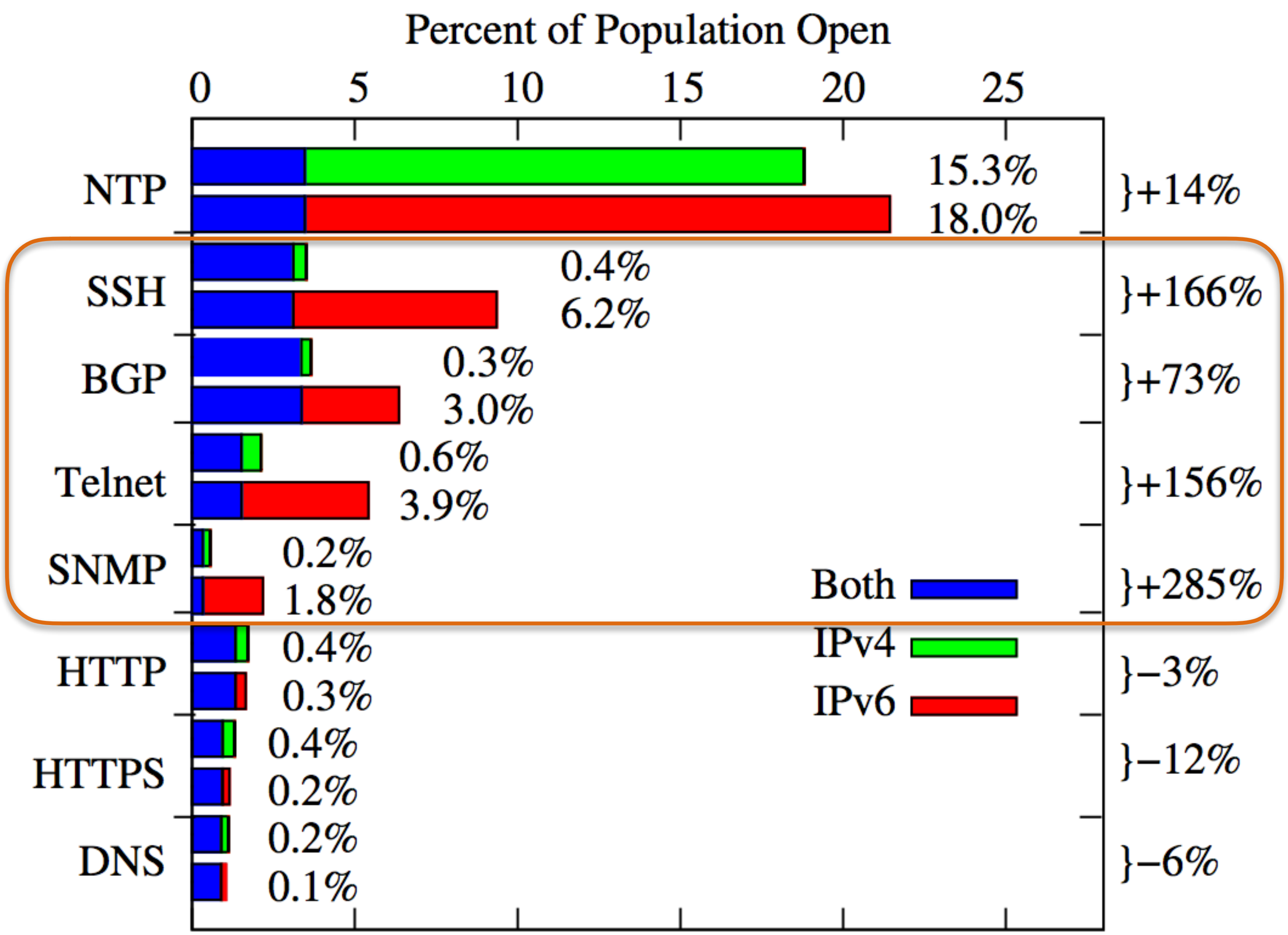
Methodology: Probing

- We use **Scamper** a parallelized network probing tool [Luckie 2010]
- Probed application ports:
  - **Routers**: ICMP echo, SSH, Telnet, HTTP, <u>BGP</u>, HTTPS, DNS, NTP, SNMPv2
  - **Servers**: ICMP echo, <u>FTP</u>, SSH, Telnet, HTTP, HTTPS, <u>SMB</u>, <u>MySQL</u>, <u>RDP</u>, DNS, NTP, SNMPv2
- Probe types (for each IP of each host against each application port):
  - **Basic** (ICMP Echo, TCP SYN, UDP request)
  - **Traceroute**-style (iterative with limited TTL/Hop Limit)
- Interpretation: probe success = ICMP echo reply, TCP SYN+ACK, UDP Data

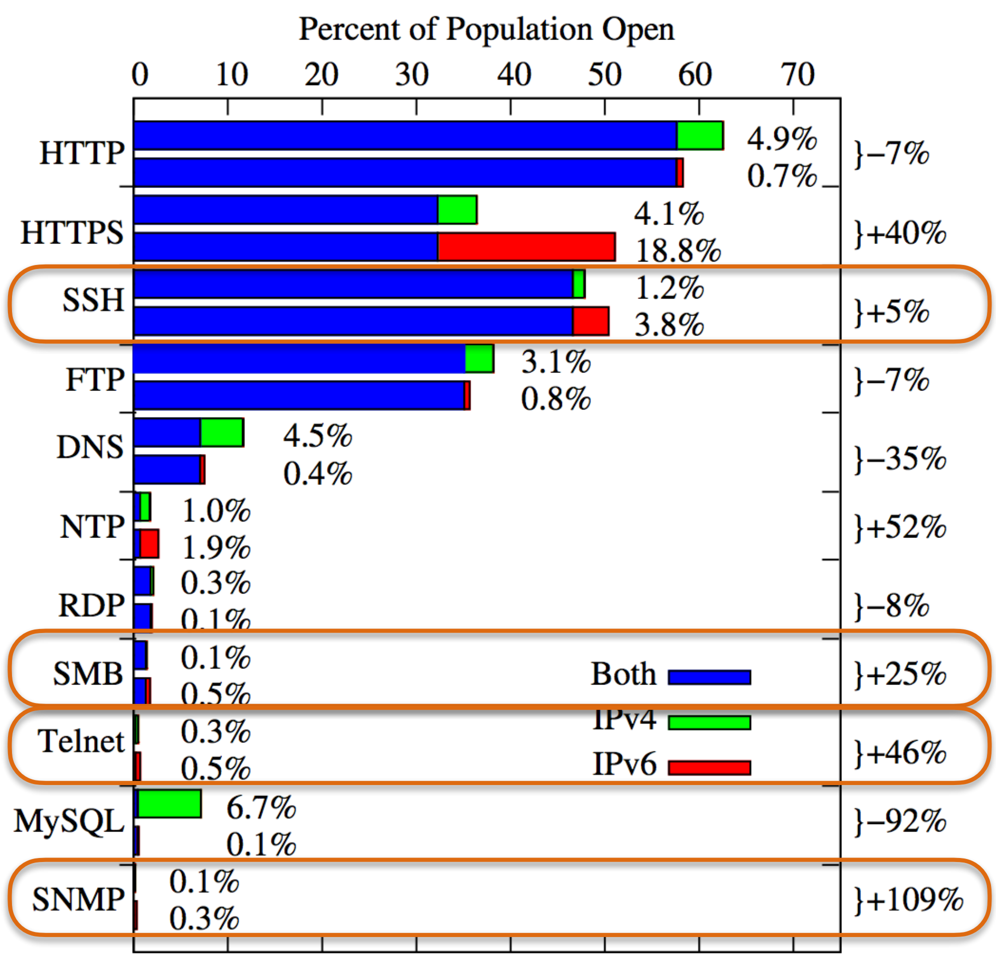
Methodology: Ethics and Best Practices

- probed at very low rate
- used standards-compliant simple packets (no fuzzing of fragment handling code :))
- signaled benign intention of traffic, e.g. via DNS name and project info website on probe IP
- respected opt-out requests + seeded opt-out list

Results: Router Openness



Results: Server Openness



(a) Servers ($\mathcal{S}_B$)

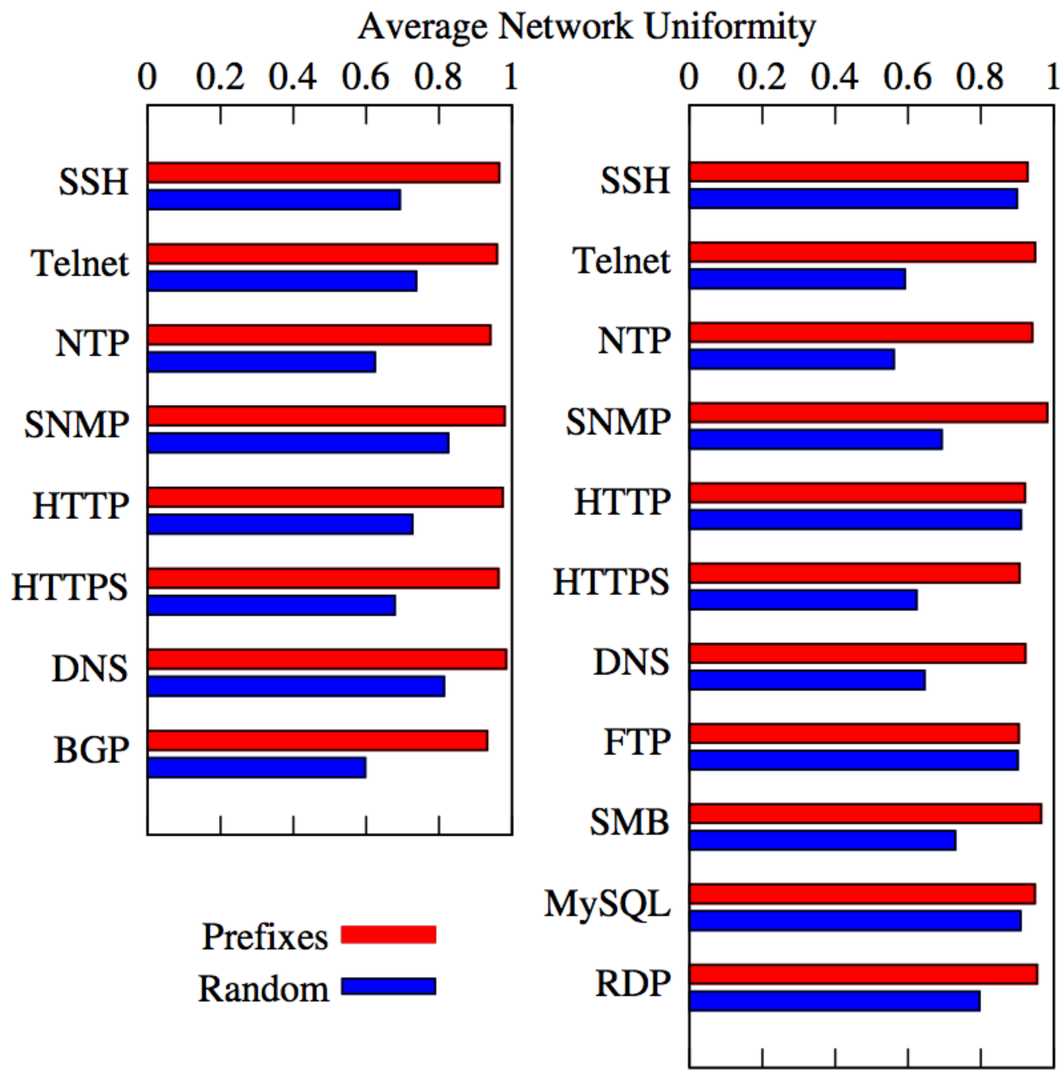
Results: Intra-Network Uniformity

Q: Are discrepancies one-offs or generally systematic security posture within network boundaries?

Uniformity metric:

For each network (routed prefix):
Across all hosts with v4 or v6 open,
find count of most common result (4,6,both)
and divide by total hosts in that network.

A: misconfigurations generally systematic within network boundaries: consistency >90%



(a) Routers

(b) Servers

Blocking Mechanism

Does the *manner* in which blocking happens differ for v6?

	Router ($\mathcal{R}_T$)		Server ($\mathcal{S}_T$)	
Mode	**Mean IPv4**	**Mean IPv6**	**Mean IPv4**	**Mean IPv6**
Open	4.17	6.04	18.57	18.89
Passive:Target	43.50	27.15	36.06	31.17
Passive:Other	10.12	15.82	16.31	14.20
Active:Target	30.93	36.14	22.82	27.61
Active:Other	3.55	6.94	2.09	2.79

Yes, there appear to be fewer policy devices (firewalls or ACLs) passively dropping requests in IPv6

Notifications & Validation

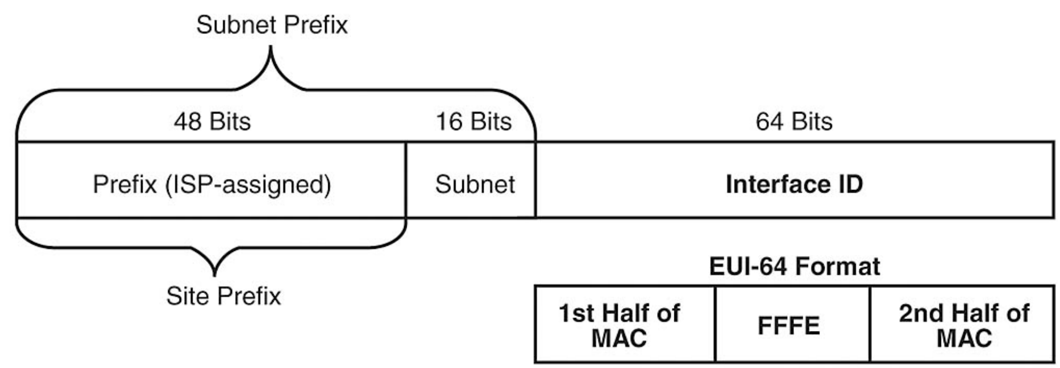
- Directly contacted 12 network operators including several with largest discrepancy
- Asked each if (1) findings were correct and (2) policy discrepancy was intentional
- All confirmed
- Post-paper full notification

Operator	Host-App Pairs w/Only IPv6 Open	Response
Global CDN 1	3	✓
Tier1 ISP 1	498	
Global Transit Pro. 1	201	✓
Large Hosting Pro. 1	≈800	
Large University 1	5	✓
Large University 2	6	✓
Large University 3	989	✓
National ISP 1	4757	✓
National ISP 2	89	
Research/Ed. ISP 1	1	✓
Research/Ed. ISP 2	523	✓
Research/Ed. ISP 3	77	✓
Research/Ed. ISP 4	17	✓
Small Hosting Pro. 1	17	✓
Small ISP 1	12	
Small Transit Pro. 1	2	✓

Scanning Feasibility

- Could brute attackers/worms discover these open IPv6 ports sans DNS?
- 128 bit address space makes global exhaustive scanning prohibitive. $O(10^{22}$ years)
- Site prefixes easily found in BGP
- Subnet IDs: Low 8 + upper 4 bits = 0.4% of space: 55-64% of subnets
- Thus, scanning individual networks (given BGP prefix lists) may be fruitful depending on interface ID assignment

128-bit Address Layout



(source: http://www.elec-intro.com/EX/05-15-08/17fig07.jpg)

Scanning Feasibility: IIDs

		Router		Server	
IID Bits Used	IID Value Range	%	Cum. %	%	Cum. %
1	<= 0x0001	23.74	23.74	5.83	5.83
4	<= 0x000F	37.89	61.63	5.94	11.77
8	<= 0x00FF	6.87	68.49	4.76	16.53
16	<= 0xFFFF	11.00	79.50	5.50	22.03
32	<= 0xFFFF FFFF	9.81	89.31	14.50	36.53
EUI-64	Middle == 0xFFFE	0.92	90.23	4.92	41.45
Other	Not in Above	9.77	100.00	58.55	100.00

- **Majority of routers and > 1/3 of servers could be found in just lower half of IID bits** (1 four billionth of the bit space!)
- Targeting one subnet using a modern scanner (zmap) at 1.4 Mpps (**1 Gbps**):
  - Instead of **418K years** for naive brute-force scan of all 64 bits **…**
  - Scanning low 32 bits + top 8 EUI-64 vendors finds: **90% of routers and 40% of servers in just 53 minutes (or just low 16 bits: 80% & 26% in 1sec.!)**

Summary and Implications

- **Large discrepancies between v4 and v6 service reachability**:
    - 43% of hosts differ on at least one application
    - 26% of hosts more open on v6 for at least one app port
- **IPv6 more open than IPv4** for high-value application ports on large Internet samples routers and servers
    - Includes **sensitive apps**: SSH, Telnet, BGP, and SNMP
- Results consistent within network boundaries: **systematic**
- Multiple evidence that **firewalls less common** on IPv6

Summary and Implications

- IPv6 is here, but basic IPv6 security has not fully arrived. **This has left thousands of routers and servers lacking basic port security.**
- Since NAT is expected to be less common with IPv6, host security is even more critical
- **What to do if you run IPv6?:**
  - **Check yourself**! (We've made a scamper module available for probing your network)
  - **Protect yourself:** Is your firewall configured for IPv6? (And effective?)
  - **Hide yourself:** Your host addressing scheme may determine IPv6 scanning feasibility. Randomly-assigned IIDs strongly suggested.

Questions?

Thank You!