

A Principled Approach to Measuring the IoT Ecosystem

Deepak Kumar

Advised By: Michael Bailey

Committee: Michael Bailey, Nikita Borisov, Adam Bates, Gang Wang, Zakir Durumeric



Internet of Things... are here!

It's 2020.



**To this point, there is little work on
measuring the network capabilities and
behaviors of IoT devices in the wild**



Challenges to IoT Measurement

Vantage Points

- Vantage Point – Where you draw the measurement from
 - Home networks: Many IoT devices are behind NATs, requiring a local network to study devices
 - Public IPv4: Public fingerprint of a device is often the only perspective researchers have for security analysis



Challenges to IoT Measurement Techniques

- Techniques – How you conduct the measurement
 - Active: Probe devices (e.g., send TCP SYN) to learn of device capabilities
 - Passive: Observe devices (e.g., network tap, darknet) to learn their behaviors

Thesis Statement: Network measurements of IoT devices drawn from an external or internal vantage point using only active or passive techniques present a biased view of network services in the IoT ecosystem.

Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

All Things Considered – Recap

- Partnered with Avast antivirus to measure IoT devices inside home networks
- Quantified the devices, vendors, and security profile of devices inside 16M homes containing 83M devices over 11 regions through active, internal scans
- IoT devices are widespread: more than half of households have at least one IoT devices in three regions, and 66% of homes in North America have at least one IoT devices
- Regions have unique device type and vendor preferences, highlighting a fractured and heterogeneous ecosystem
- 67.5% of IoT devices supported at least one TCP- or UDP- based service based on active probing

Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

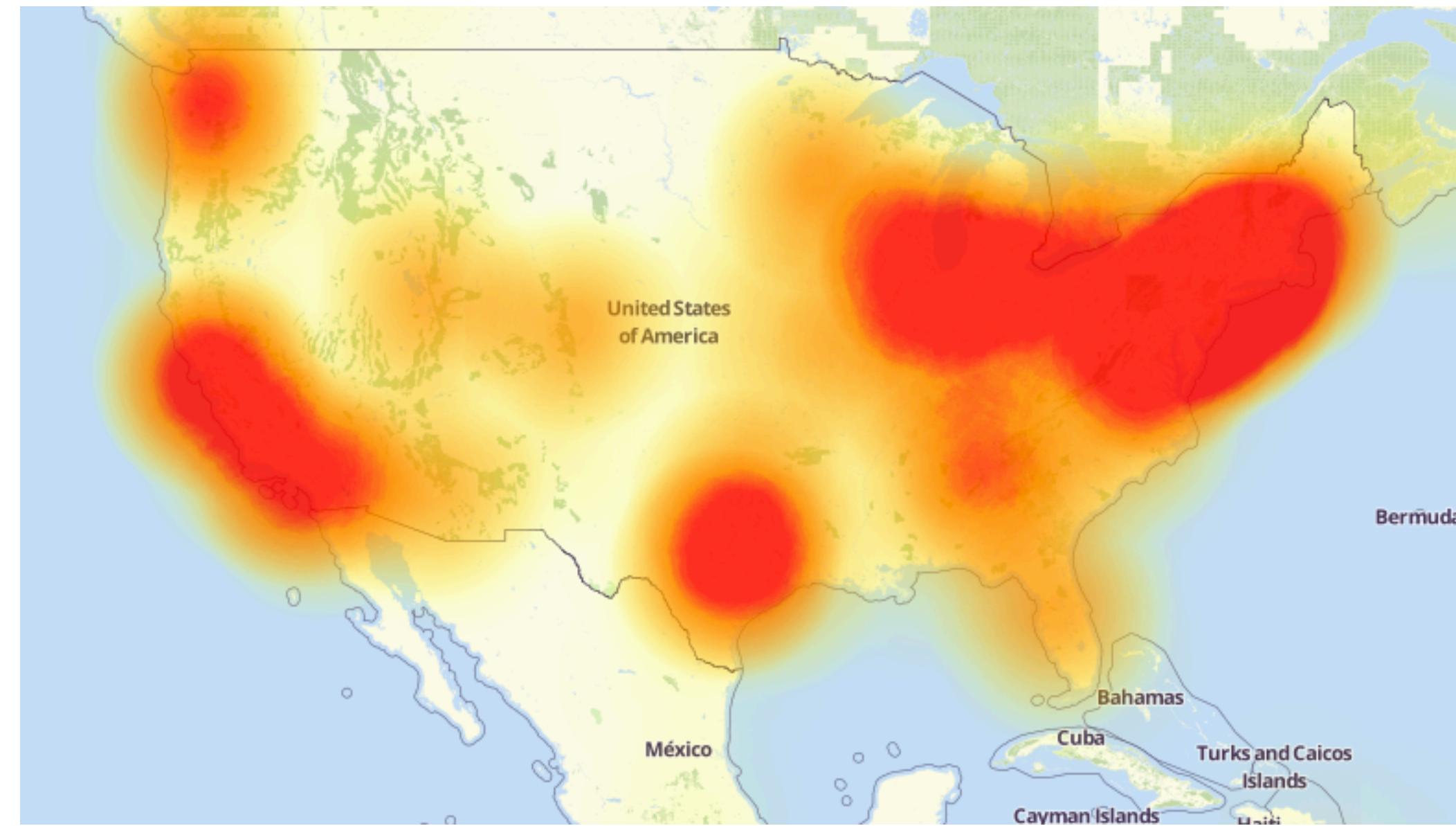
Cyberattack Knocks Out Access to Websites

Popular sites such as Twitter, Netflix and PayPal were unreachable for part of the day

Here are the 61 passwords that powered the Mirai IoT botnet

That time your smart toaster broke the internet

How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet



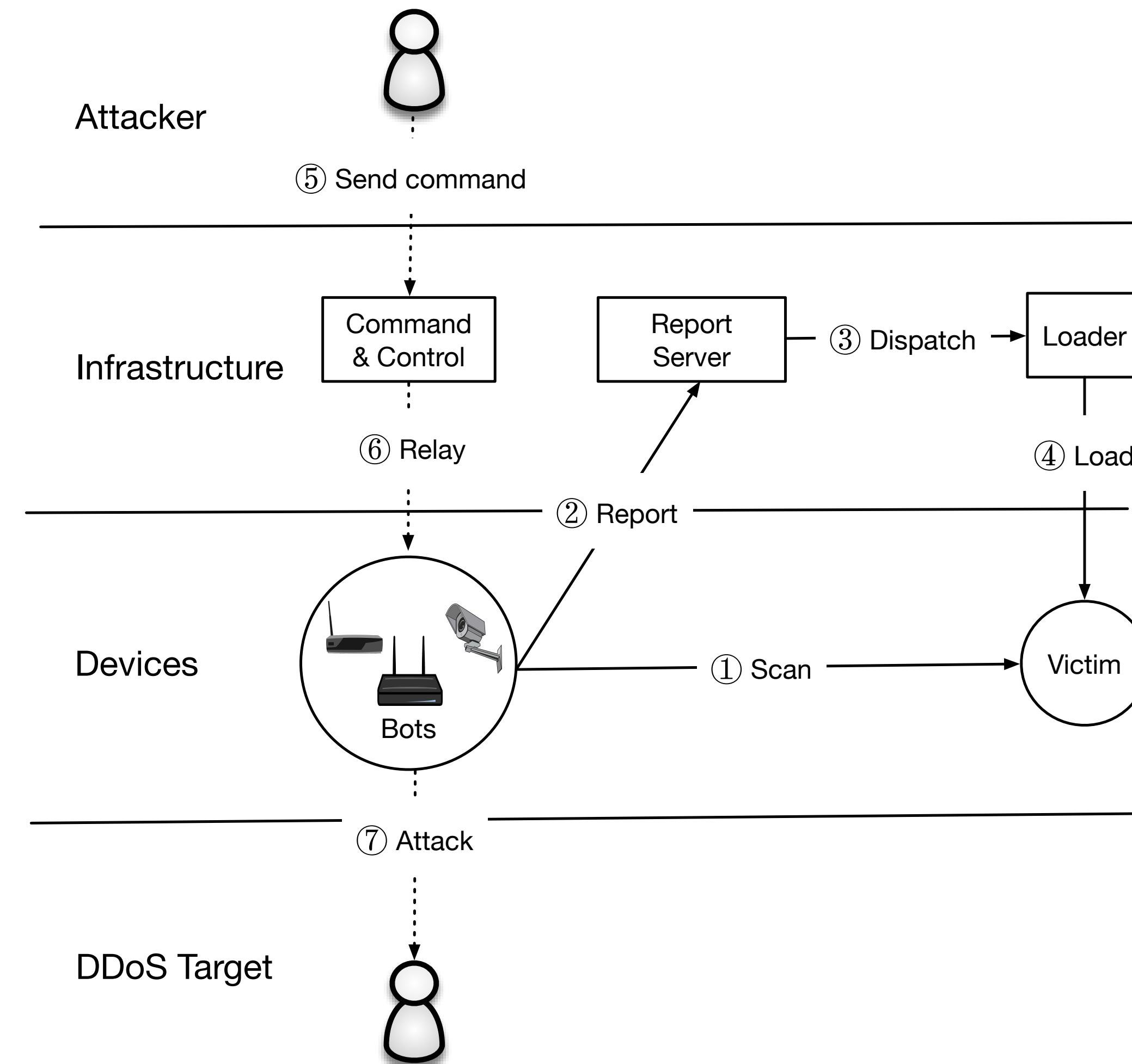
Studying the Mirai Botnet

Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	136 IPv4 scans
Telnet Honeypots	434 binaries
Malware Repository	594 binaries
Active/Passive DNS	499M Daily RRs
C2 Milkers	64K issued attacks
Krebs DDoS Attack	170K attacker IPs
Dyn DDoS Attack	108K attacker IPs

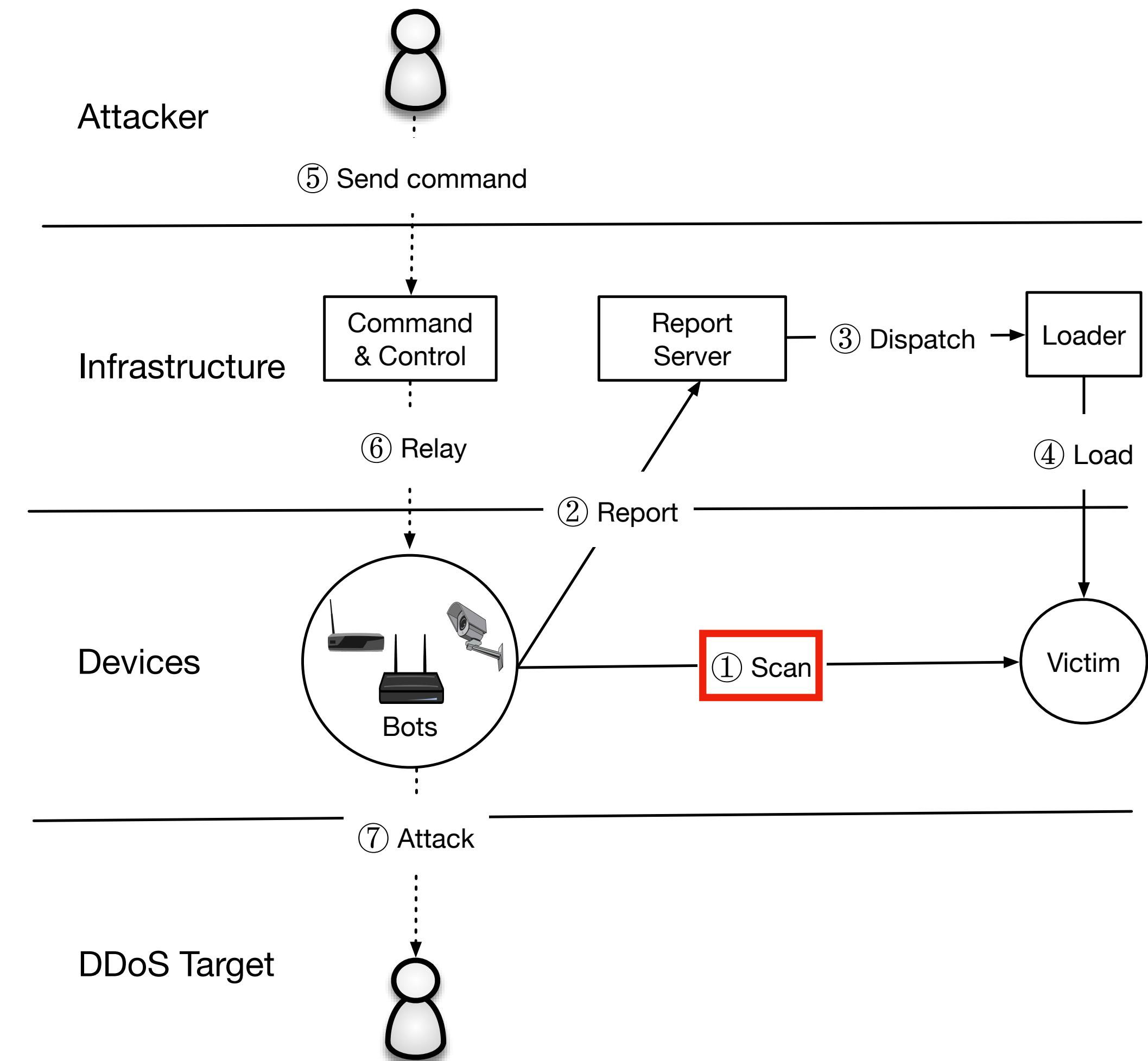
Studying the Mirai Botnet

Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	136 IPv4 scans
Telnet Honeypots	434 binaries
Malware Repository	594 binaries
Active/Passive DNS	499M Daily RRs
C2 Milkers	64K issued attacks
Krebs DDoS Attack	170K attacker IPs
Dyn DDoS Attack	108K attacker IPs

How Did Mirai Work?



How Did Mirai Work?



What Devices did Mirai Infect?



Active, External Scanning for Device Identification

- We leveraged active, external scans from Censys for five application layer protocols
- Our passive darknet identified 1.2M IP addresses that were scanning with the Mirai signature with 1.8M banners total
- Used regular expressions generated by Nmap project and custom rules for HTTPS, CWMP
- Identified either the device type, model, or vendor for 31.5% of IPs

Protocol	Banners	Devices Identified
HTTPS	342K	271K (79.4%)
FTP	320K	144K (45.1%)
Telnet	473K	104K (22%)
CWMP	506K	35K (7%)
SSH	150K	8K (5.5%)
Total	1.8M	588K (31.5%)

Identified Devices

CWMP	Telnet	HTTPS	FTP	SSH
Router (4.7%)	Router (17.4%)	Camera/DVR (36.8%)	Router (49.5%)	Router (4%)
	Camera/DVR (9.4%)	Router (6.3%)	Storage (1%)	Storage (0.2%)
		Storage (0.2%)	Camera/DVR (0.4%)	
		Other (0.3%)	Media (0.1%)	
Unknown (95.3%)	Unknown (73.1%)	Unknown (56.4%)	Unknown (49%)	Unknown (95.6%)

How does this compare to an external vantage point?

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Comparing Active Internal and Active External

- Collected IoT devices from Avast and Censys active scans on a single day, May 2, 2020
- Performed external device type identification using five protocols: HTTPS, CWMP, Telnet, SSH, FTP
- CWMP, Telnet most descriptive (by label), while HTTPS, CWMP offered on most devices
- Labeled 6.1M external IoT devices, 1.8M internal IoT devices

Protocol	% IPv4 Responded	% IPs Labeled
443/HTTPS	38.3%	3.7%
7547/CWMP	19.3%	16.3%
22/SSH	16%	2.4%
21/FTP	9.1%	6.8%
23/Telnet	2.4%	20.6%

Comparing Active Internal and Active External

Service	Protocol	Internal Rank	External Rank
80	HTTP	1 (72%)	3 (15.9%)
53	DNS	2 (37%)	8 (3%)
443	HTTPS	3 (30%)	2 (27%)
8080	HTTP	4 (14.5%)	7 (5.8%)
22	SSH	5 (12%)	6 (7%)
631	IPP	6 (10%)	12 (0.35%)

Service	Protocol	Internal Rank	External Rank
23	Telnet	7 (8.3%)	5 (9.2%)
21	FTP	8 (7.4%)	4 (11.6%)
7547	CWMP	9 (3.9%)	1 (59%)
8888	HTTP	10 (2.4%)	14 (0.3%)
8883	MQTT	11 (1.6%)	37 (0%)

Comparing Active Internal and Active External

Service	Protocol	Internal Rank	External Rank
80	HTTP	1 (72%)	3 (15.9%)
53	DNS	2 (37%)	8 (3%)
443	HTTPS	3 (30%)	2 (27%)
8080	HTTP	4 (14.5%)	7 (5.8%)
22	SSH	5 (12%)	6 (7%)
631	IPP	6 (10%)	12 (0.35%)

Service	Protocol	Internal Rank	External Rank
23	Telnet	7 (8.3%)	5 (9.2%)
21	FTP	8 (7.4%)	4 (11.6%)
7547	CWMP	9 (3.9%)	1 (59%)
8888	HTTP	10 (2.4%)	14 (0.3%)
8883	MQTT	11 (1.6%)	37 (0%)

Comparing Active Internal and Active External

Service	Protocol	Internal Rank	External Rank
80	HTTP	1 (72%)	3 (15.9%)
53	DNS	2 (37%)	8 (3%)
443	HTTPS	3 (30%)	2 (27%)
8080	HTTP	4 (14.5%)	7 (5.8%)
22	SSH	5 (12%)	6 (7%)
631	IPP	6 (10%)	12 (0.35%)

Service	Protocol	Internal Rank	External Rank
23	Telnet	7 (8.3%)	5 (9.2%)
21	FTP	8 (7.4%)	4 (11.6%)
7547	CWMP	9 (3.9%)	1 (59%)
8888	HTTP	10 (2.4%)	14 (0.3%)
8883	MQTT	11 (1.6%)	37 (0%)

Comparing Active Internal and Active External

Service	Protocol	Avast Rank	Censys Rank
80	HTTP	1 (72%)	3 (15.9%)
23	DNS	2 (37%)	3 (23%)
443	HTTPS	3 (27%)	2 (27%)
8080	HTTP	4 (14.5%)	7 (5.8%)
445	SMB	5 (13%)	11 (0.4%)
22	SSH	6 (12%)	6 (7%)
631	IPP	7 (10%)	12 (0.35%)

Service	Protocol	Avast Rank	Censys Rank
7547	CWMP	10 (3.9%)	1 (59%)
8888	HTTP	11 (2.4%)	14 (0.3%)
8883	MQTT	12 (1.6%)	37 (0%)

The services offered by the externally available IoT ecosystem differ from those offered by the internally available IoT ecosystem

Comparing Active Internal and Active External

Device Type	% Internal Devices	% External Devices
Router	61.9%	92.3%
Media	20.7%	1.5%
Work Appliances	6.7%	0.7%
Camera	3.4%	0.6%
Generic IoT	1.1%	0.4%
Storage	0.9%	4.3%

Comparing Active Internal and Active External

Device Type	% Internal Devices	% External Devices
Router	61.9%	92.3%
Media	20.7%	1.5%
Work Appliances	6.7%	0.7%
Camera	3.4%	0.6%
Generic IoT	1.1%	0.4%
Storage	0.9%	4.3%

Comparing Active Internal and Active External Devices that support SSH

SSH	
Internal	External
Router (88.3%)	Router (97.9%)
Storage (4.2%)	Generic IoT (0.2%)
Work (3.2%)	
Camera (2%)	
Media (1.4%)	

Comparing Active Internal and Active External Devices that support HTTPS

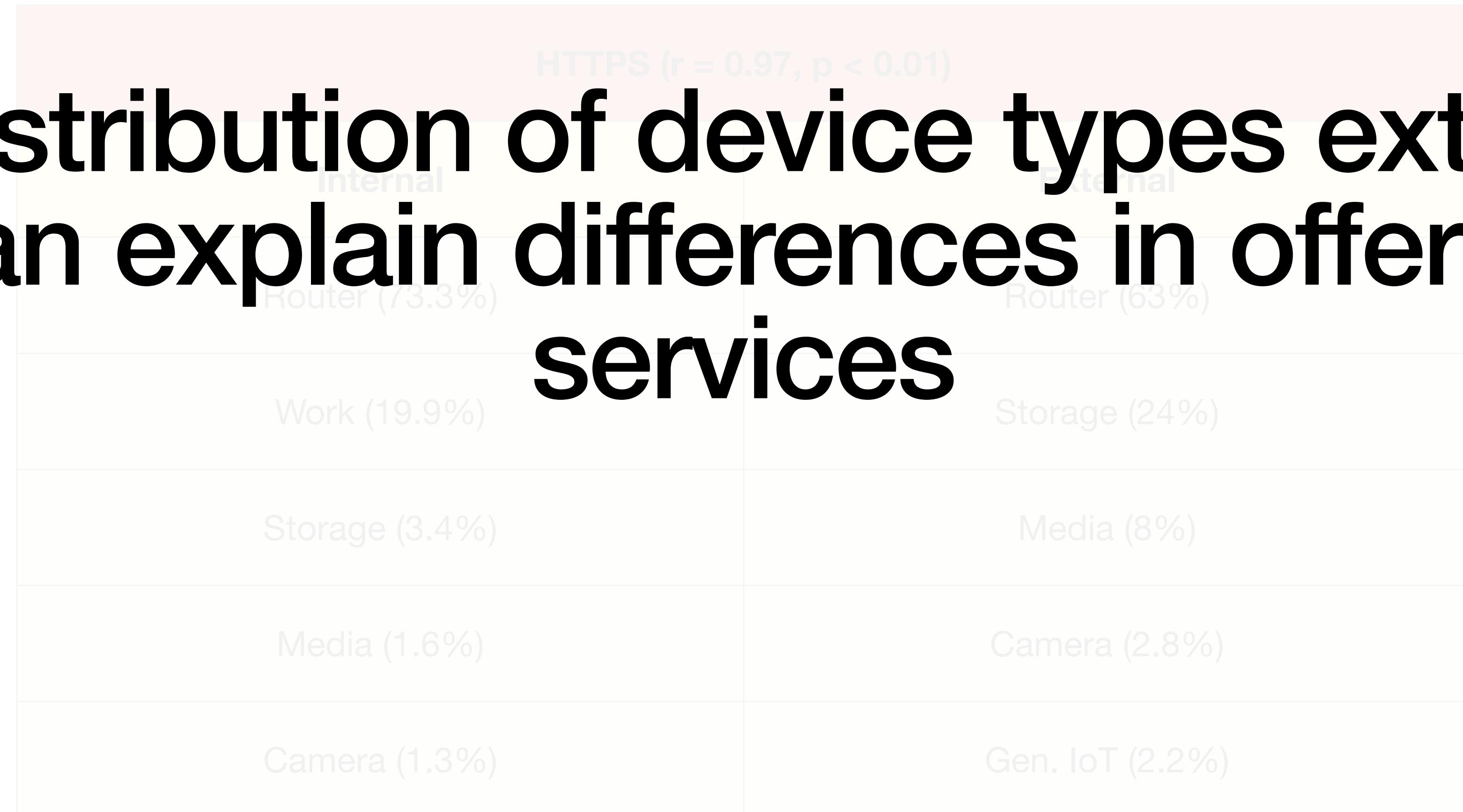
HTTPS ($r = 0.97, p < 0.01$)	
Internal	External
Router (73.3%)	Router (63%)
Work (19.9%)	Storage (24%)
Storage (3.4%)	Media (8%)
Media (1.6%)	Camera (2.8%)
Camera (1.3%)	Gen. IoT (2.2%)

Comparing Active Internal and Active External Devices that support HTTPS

HTTPS ($r = 0.97, p < 0.01$)	
Internal	External
Router (73.3%)	Router (63%)
Work (19.9%)	Storage (24%)
Storage (3.4%)	Media (8%)
Media (1.6%)	Camera (2.8%)
Camera (1.3%)	Gen. IoT (2.2%)

Comparing Active Internal and Active External Devices that support HTTPS

The distribution of device types externally can explain differences in offered services

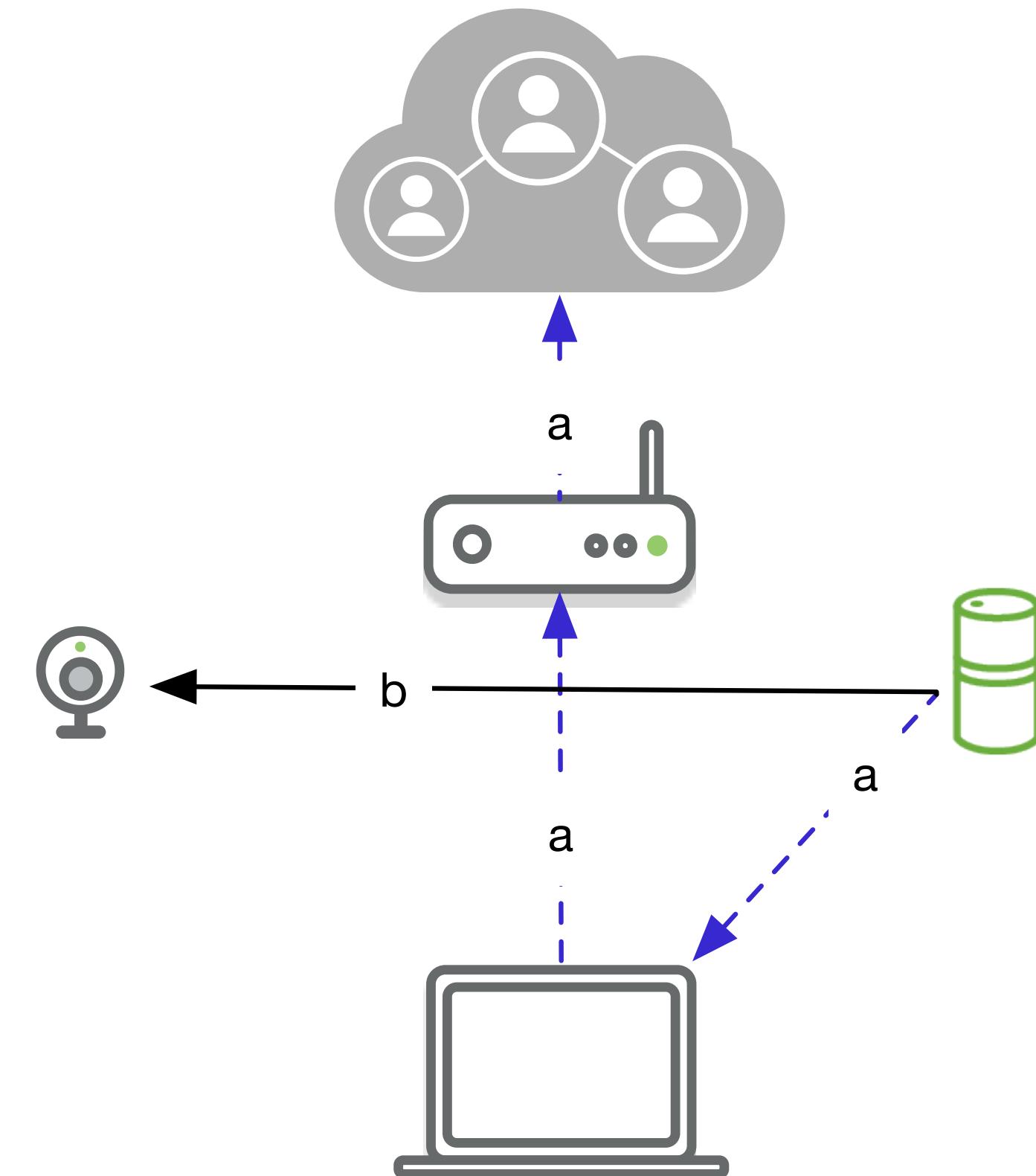


Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

IoT Inspector

- Princeton IoT Inspector is an open source tool that inspects IoT device communication to outside world to drive security and privacy insight
- Works by setting itself up as a voluntary man-in-the-middle between all devices and the gateway, logs aggregate traffic
- Design and usage approved usage by IRB



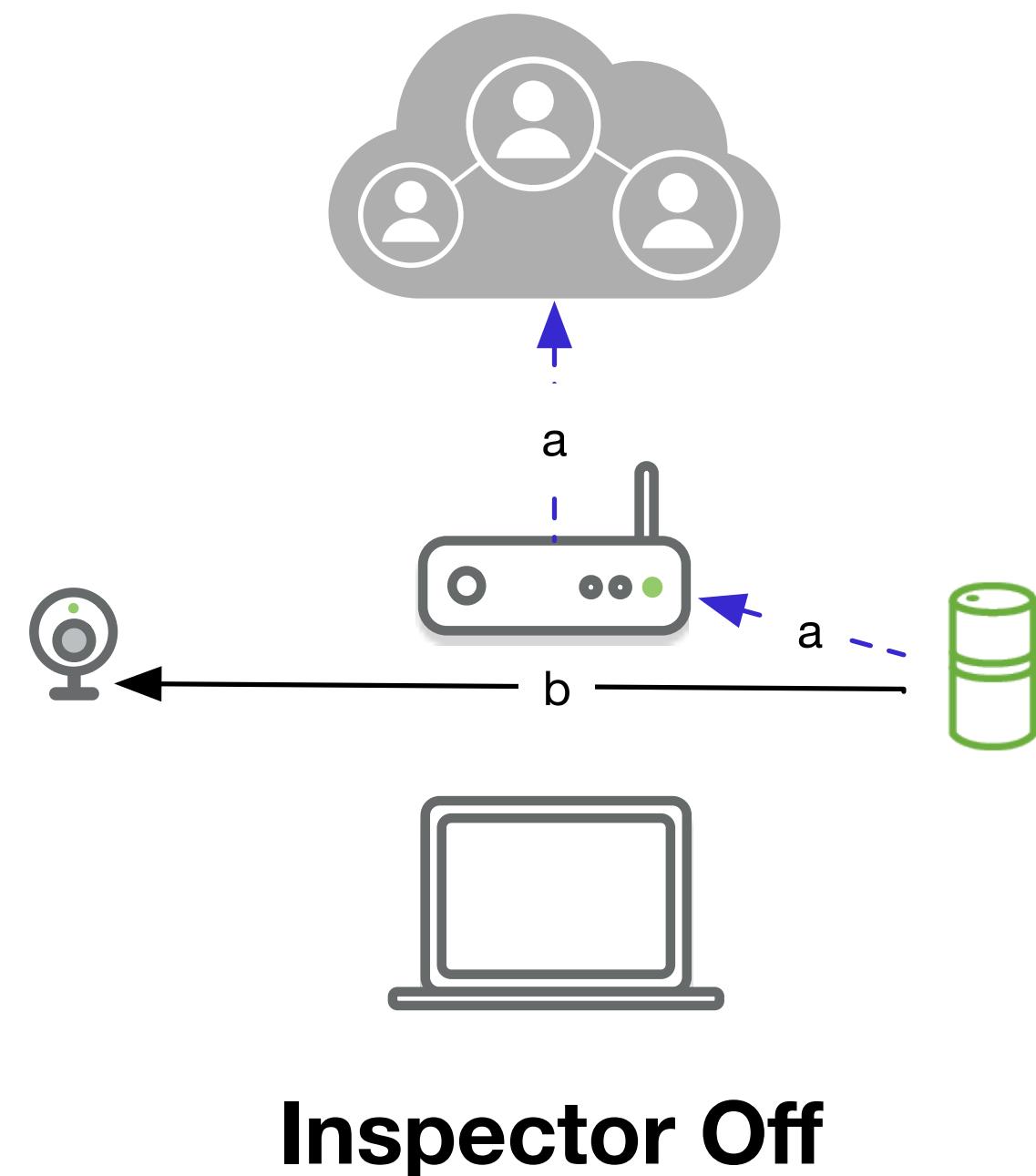
Example inspection

Instrumenting IoT Inspector

- Added ability to passively observe traffic between all devices and actively probed devices for services

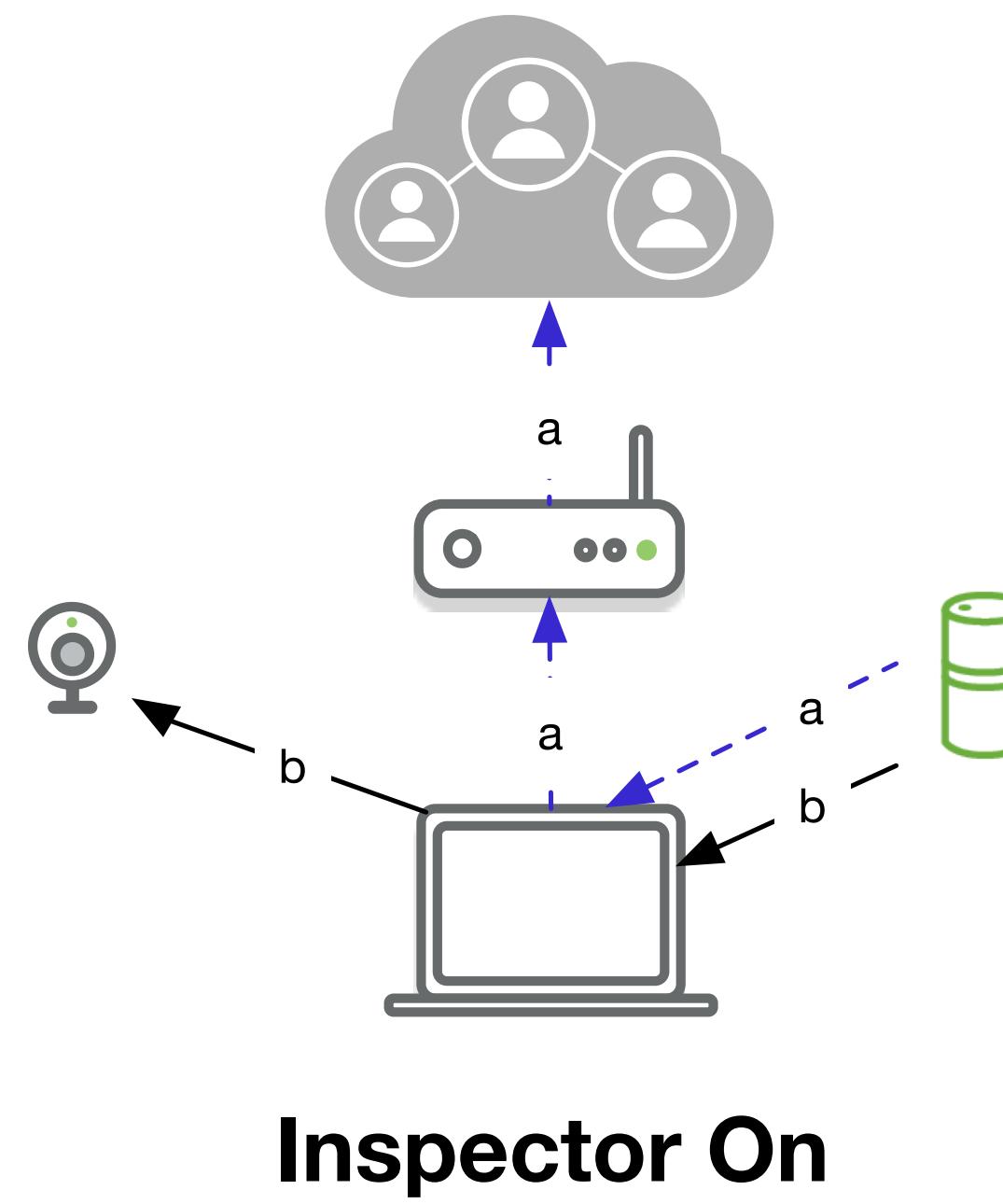
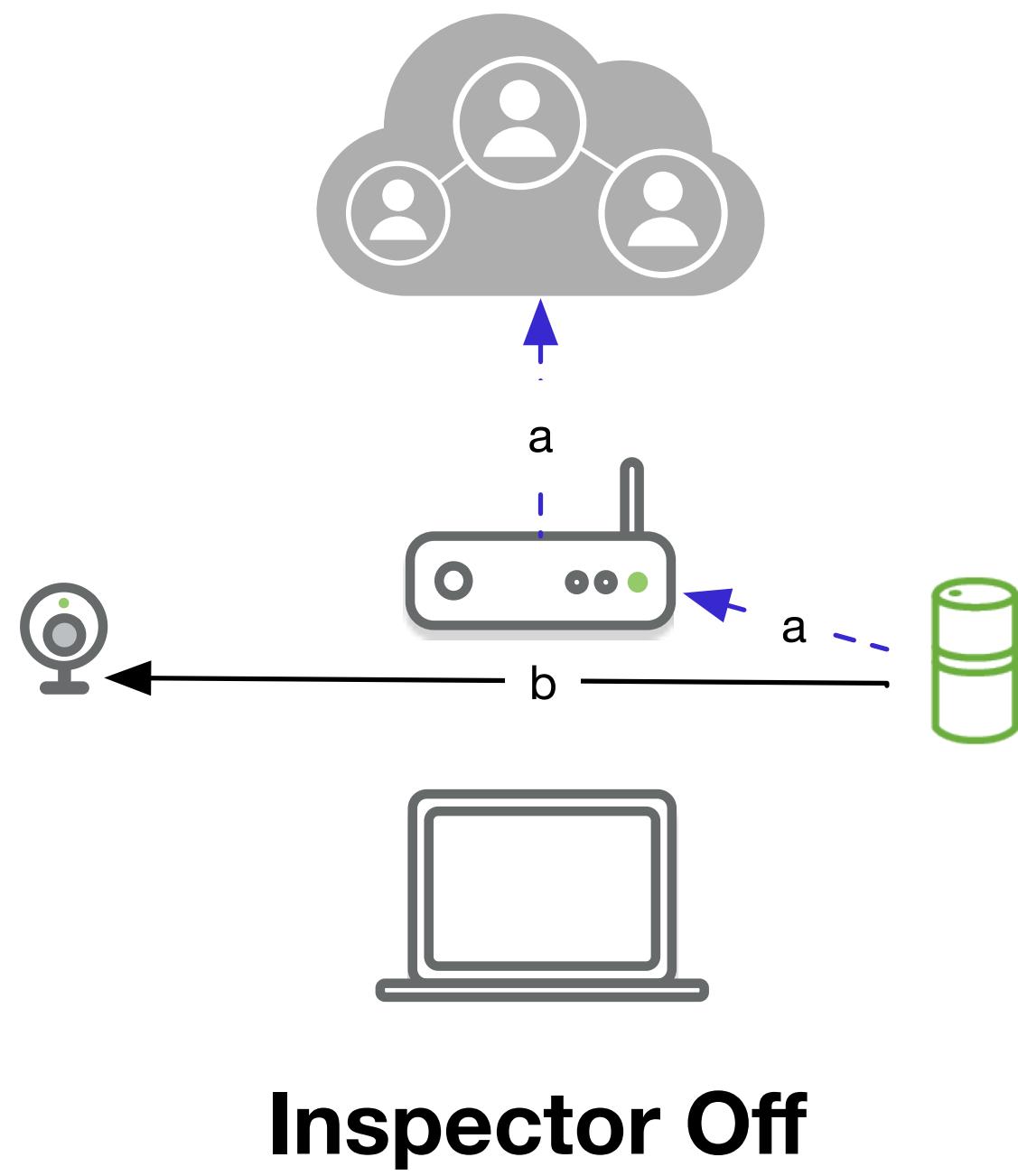
Instrumenting IoT Inspector

- Added ability to passively observe traffic between all devices and actively probed devices for services



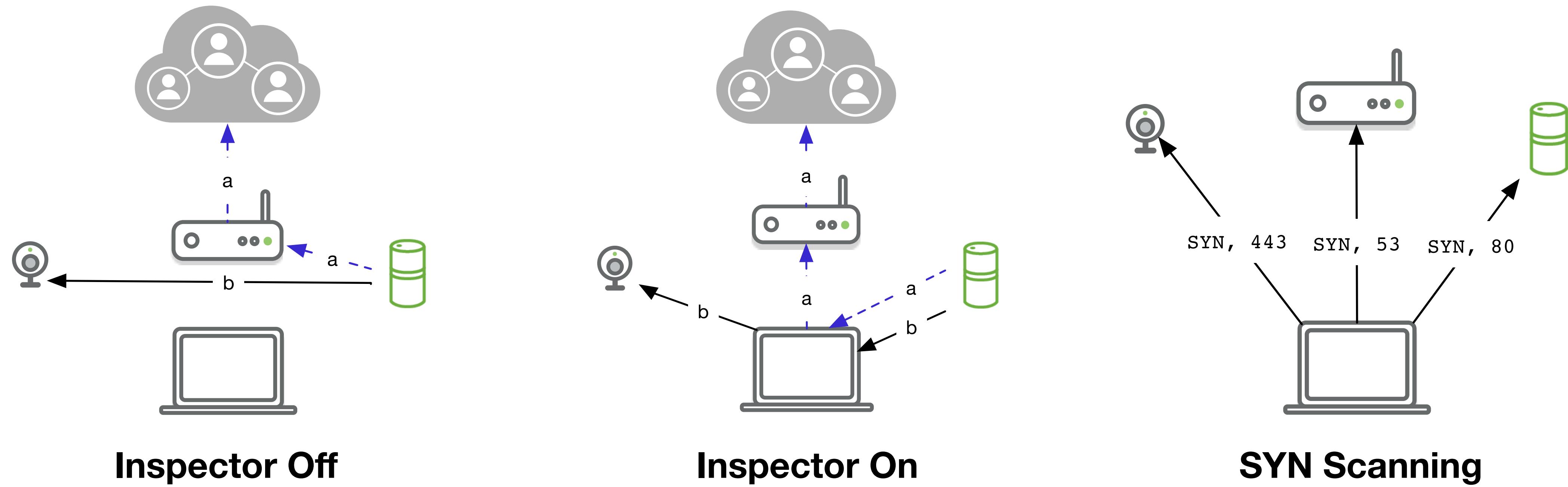
Instrumenting IoT Inspector

- Added ability to passively observe traffic between all devices and actively probed devices for services



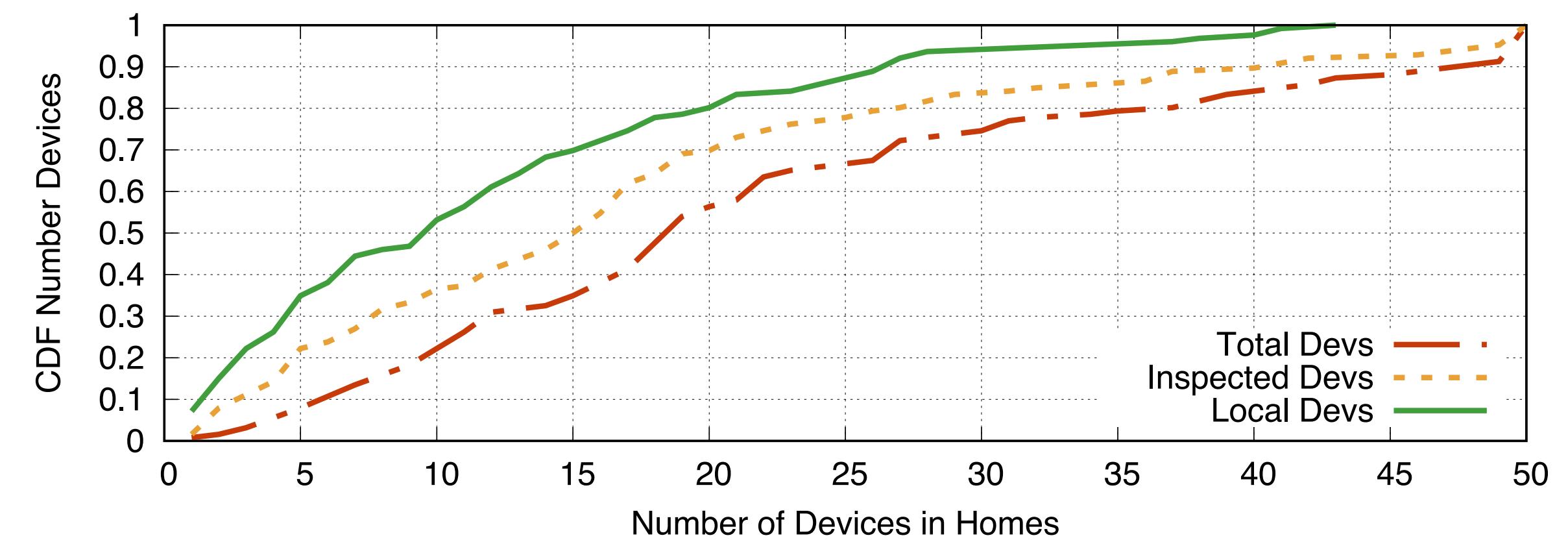
Instrumenting IoT Inspector

- Added ability to passively observe traffic between all devices and actively probed devices for services



Passive Dataset

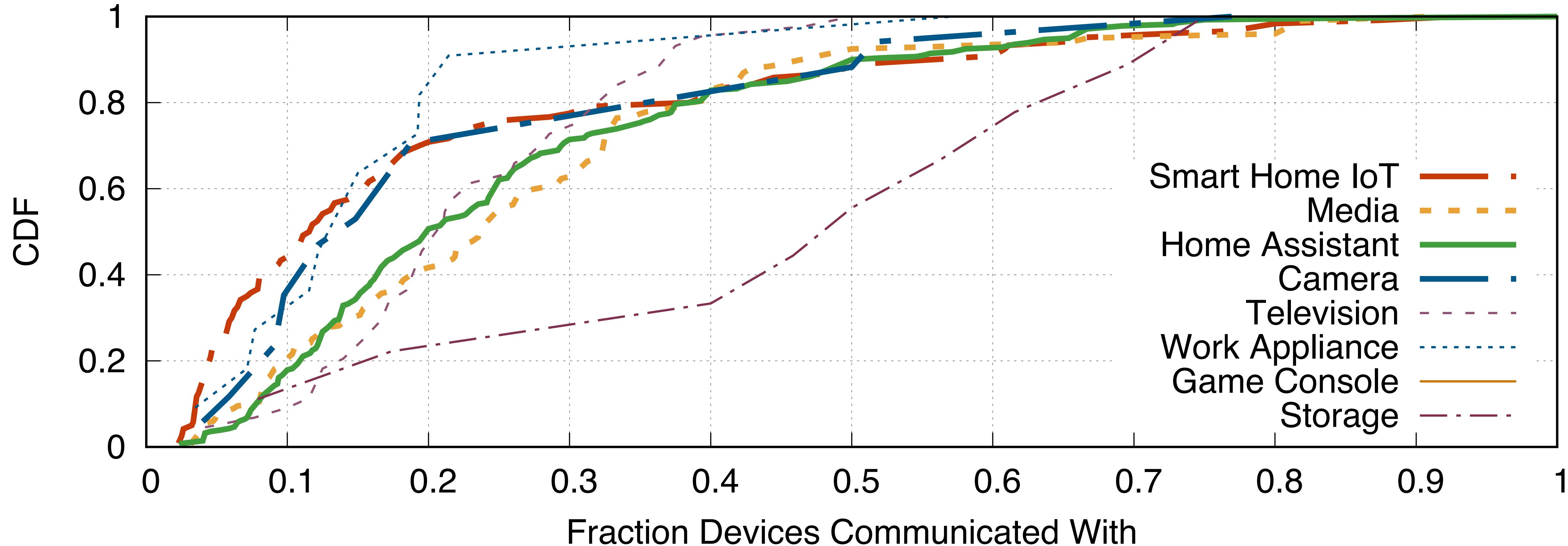
- Recruited 275 participants to run our augmented version of IoT Inspector for a 3-week period, May 8 – May 31st, 2020 in their smart homes
- 3,308 inspected devices, 2365 IoT devices
 - Used fingerbank.org for device identification, which is based on active probing and ML
- Homes in our dataset contain median 19 devices



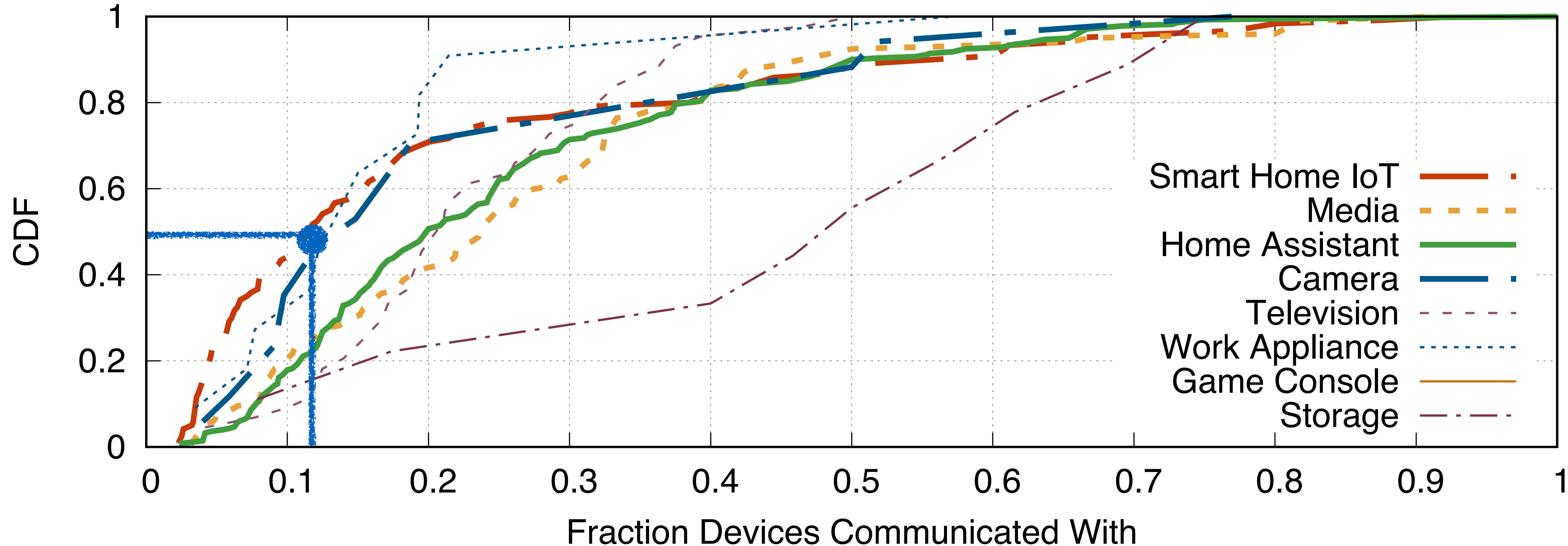
How do devices behave on local networks?



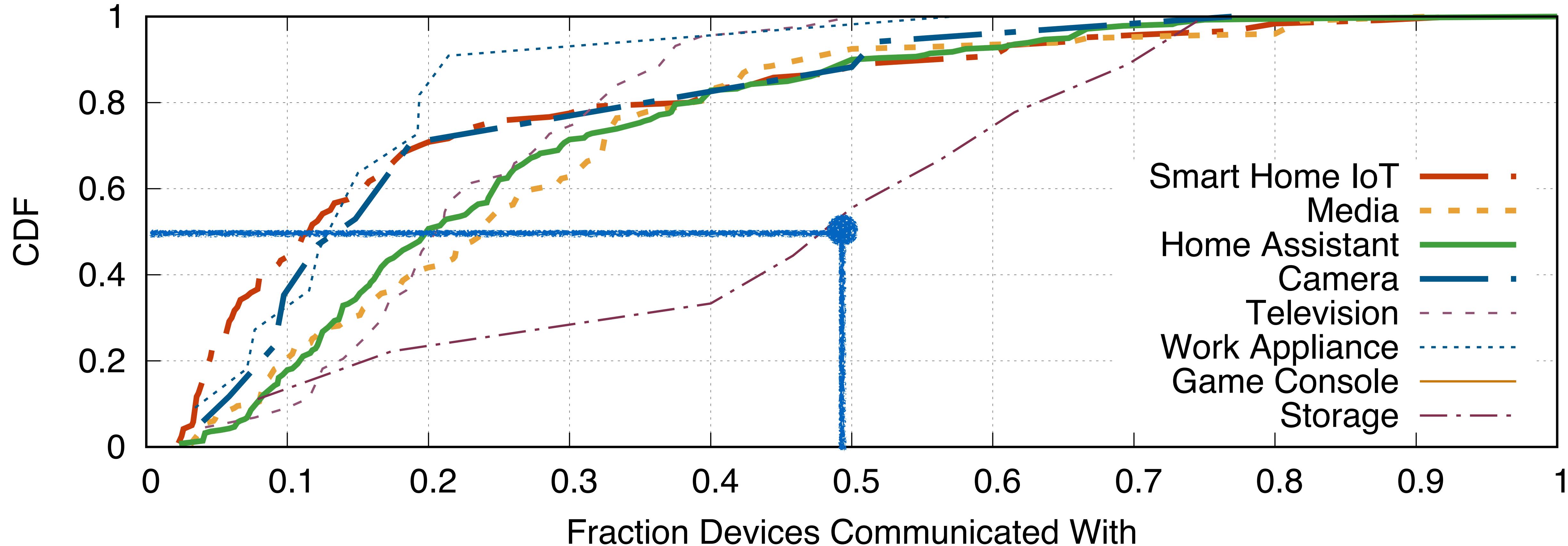
Fraction of Device Communication



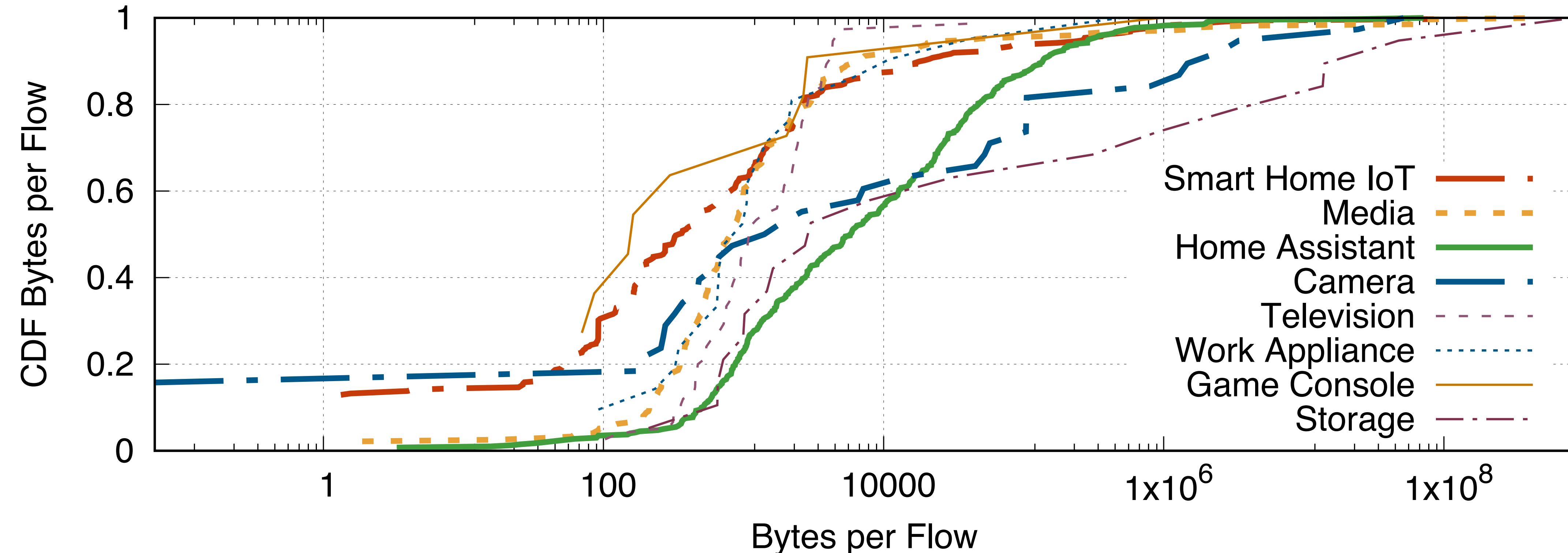
Fraction of Device Communication



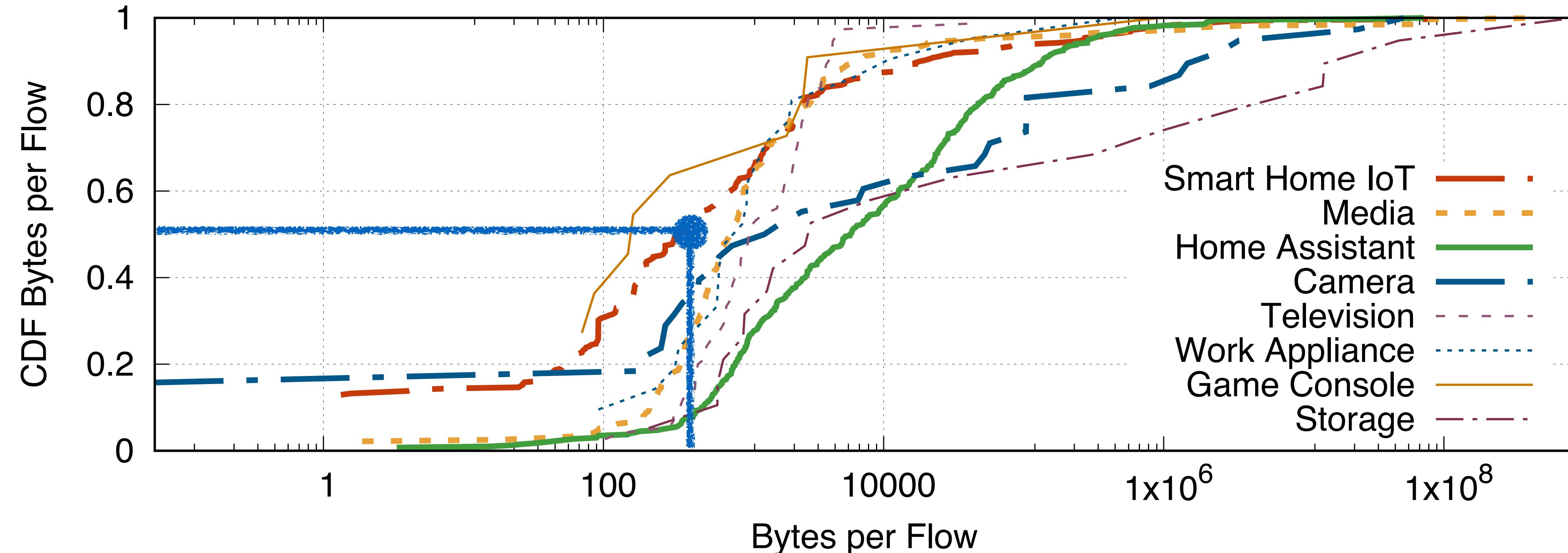
Fraction of Device Communication



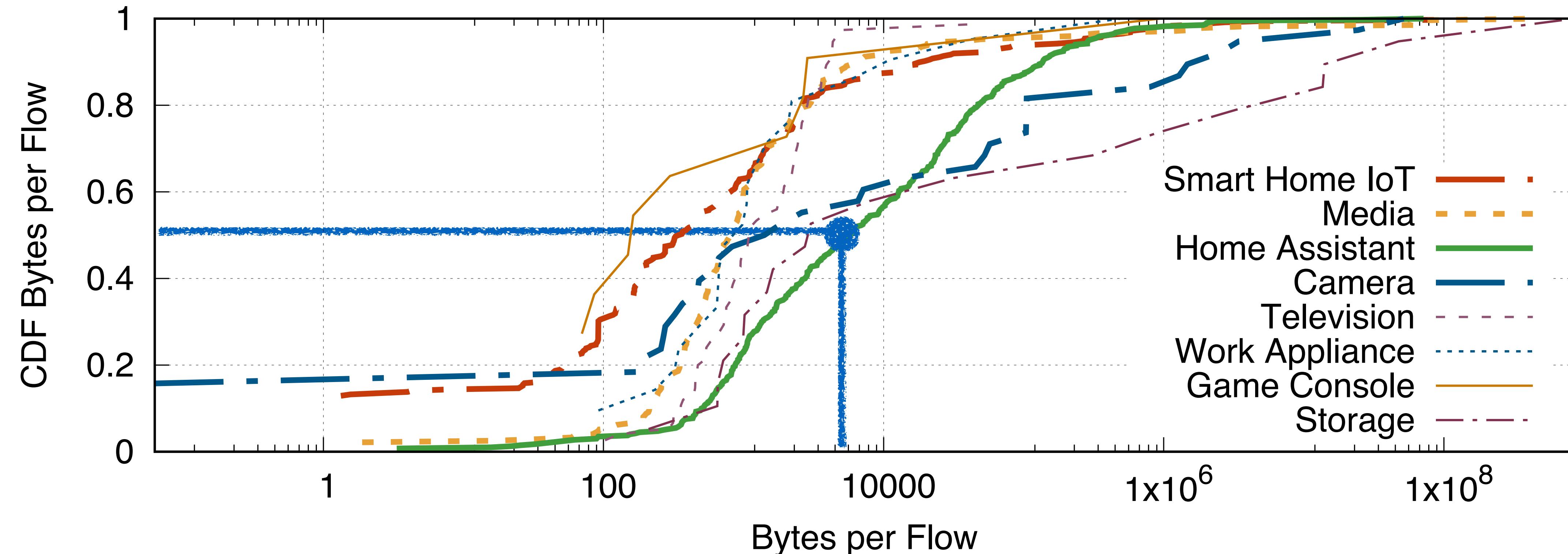
Bytes sent per flow



Bytes sent per flow



Bytes sent per flow



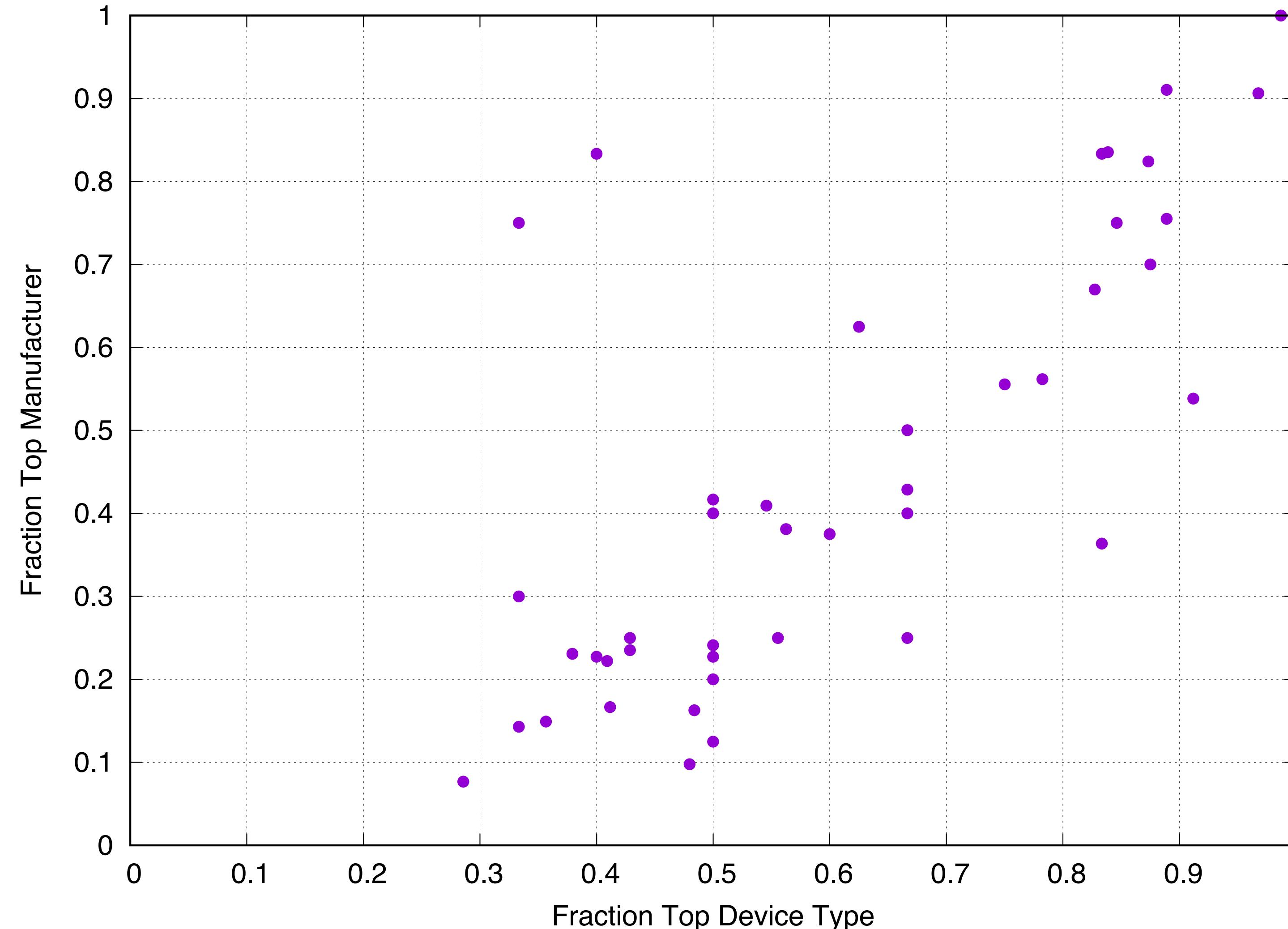
Port Usage by Fraction of Devices

Port	Protocol	Service	% Devices
8009	TCP	HTTP	12.5%
80	TCP	HTTP	9.9%
1400	TCP	HTTP	4.8%
10001	UDP	—	4.6%
8008	TCP	HTTP	4.4%
9000	TCP	—	2.9%
8060	TCP	HTTP	2.2%
10001	TCP	—	2.0%
55443	TCP	—	2.0%
161	UDP	SNMP	1.9%

Port Usage by Fraction of Devices

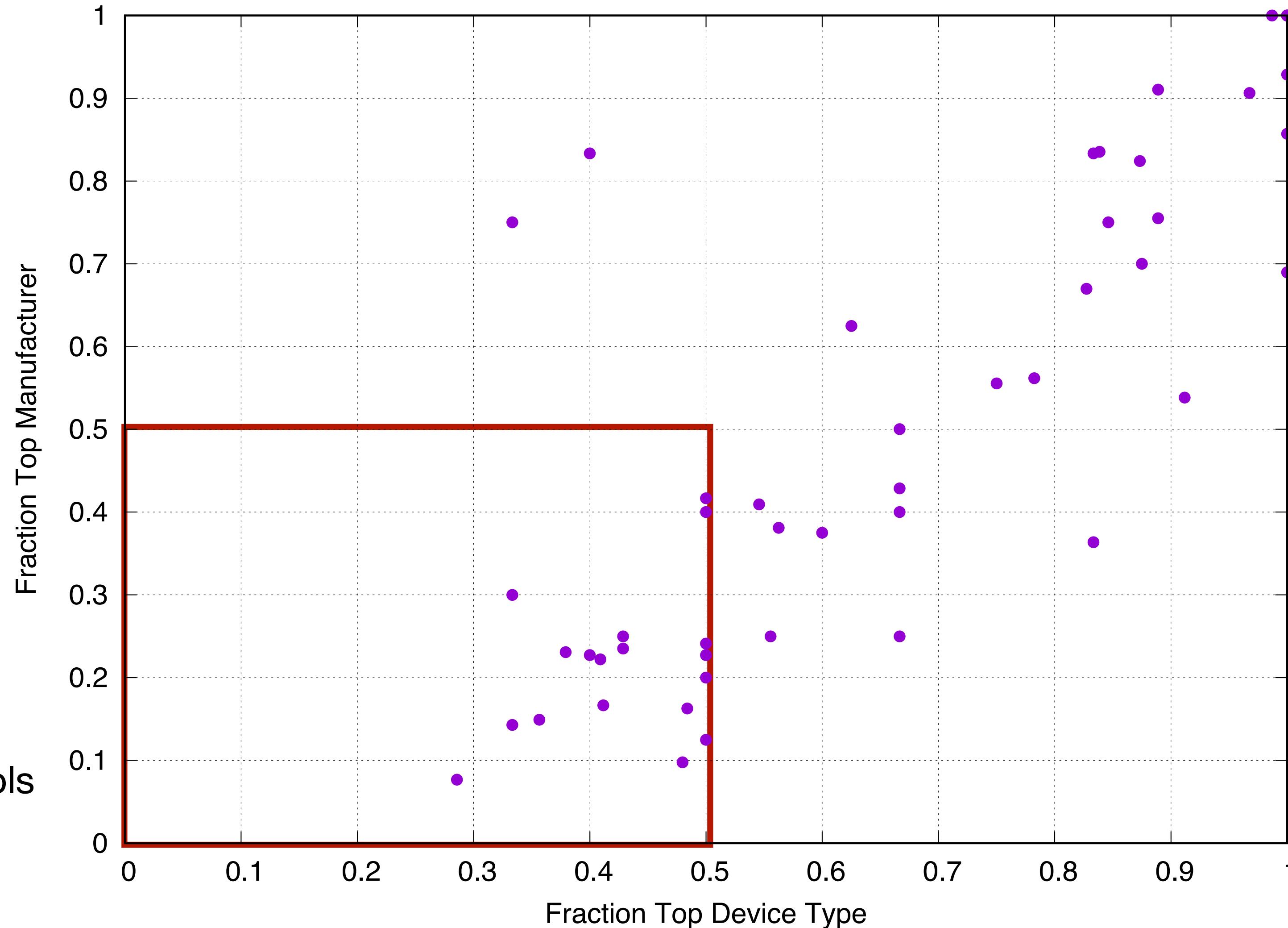
Port	Protocol	Service	% Devices
8009	TCP	HTTP	12.5%
80	TCP	HTTP	9.9%
1400	TCP	HTTP	4.8%
10001	UDP	—	4.6%
8008	TCP	HTTP	4.4%
9000	TCP	—	2.9%
8060	TCP	HTTP	2.2%
10001	TCP	—	2.0%
55443	TCP	—	2.0%
161	UDP	SNMP	1.9%

Port Distributions

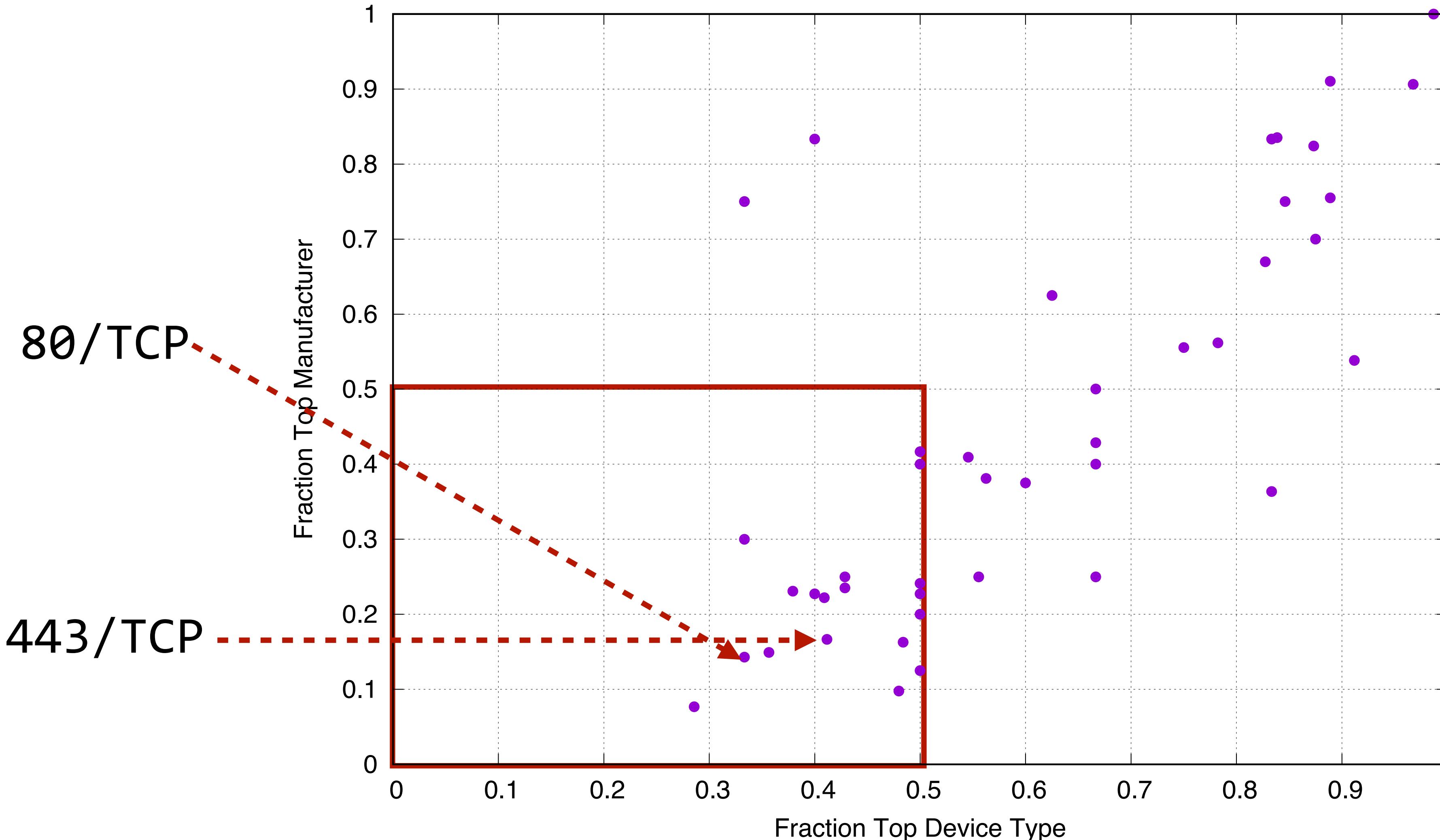


Port Distributions

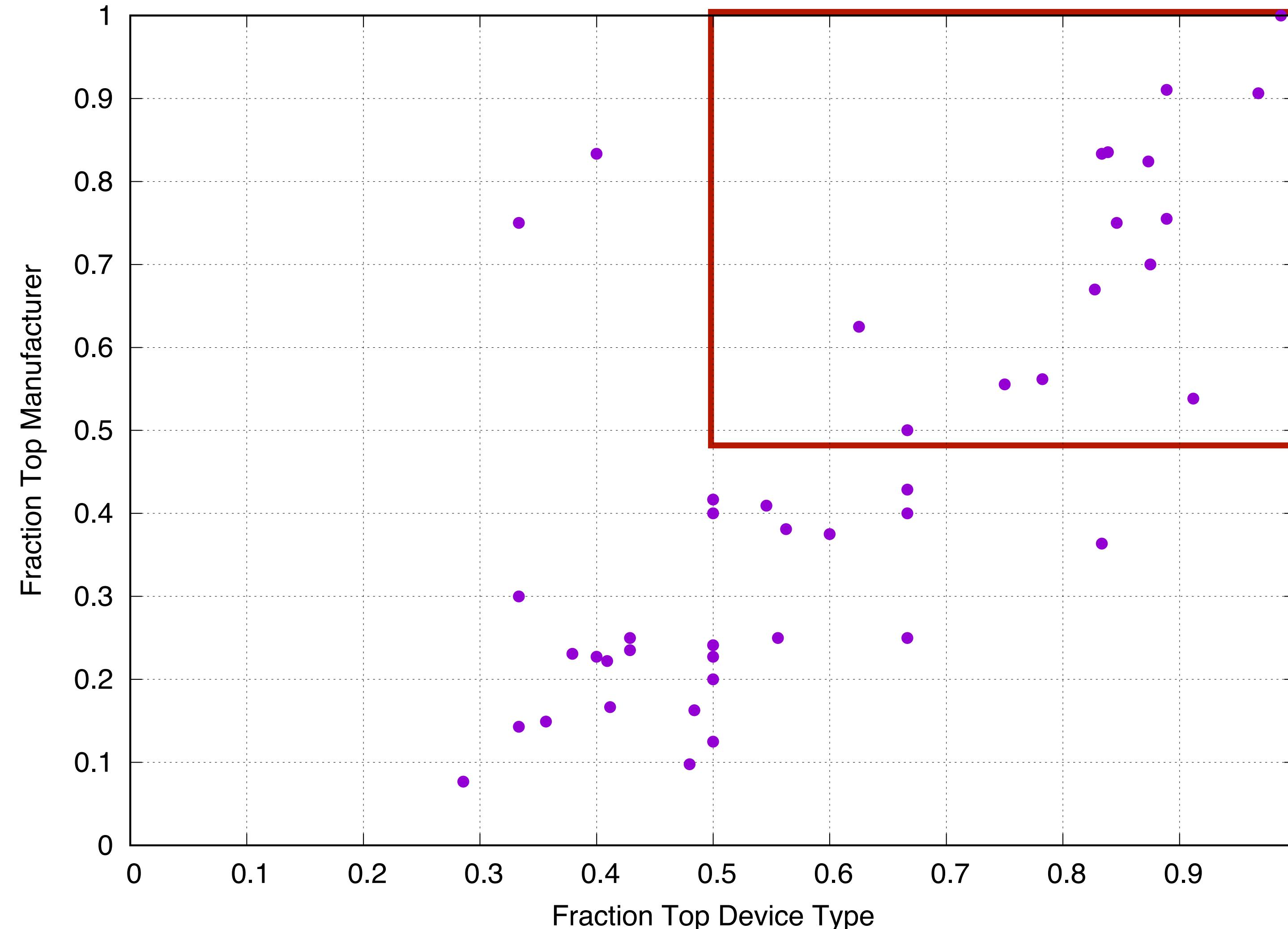
24% ports are shared by many manufacturers and device types – these are standard ports and protocols



Port Distributions

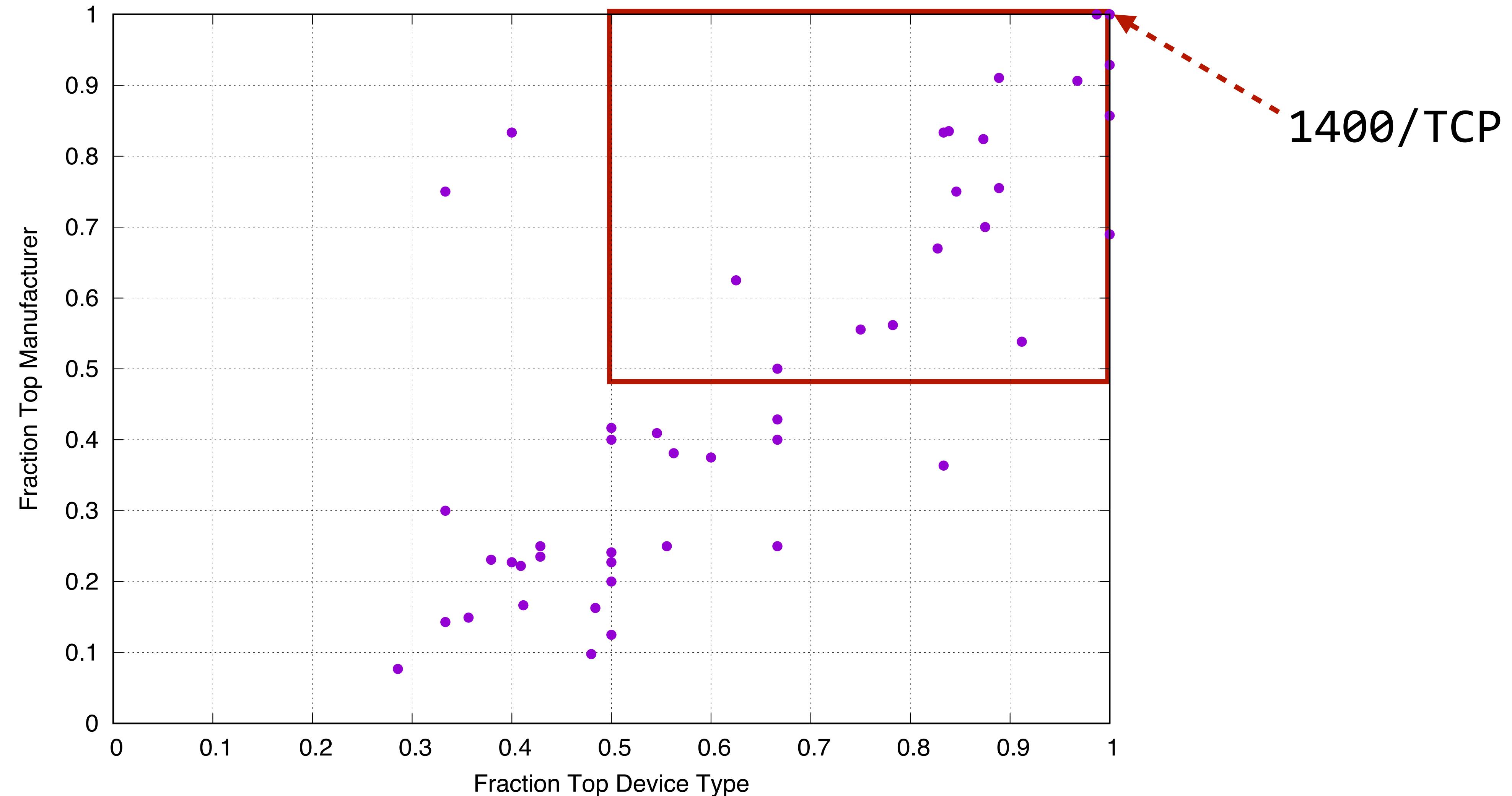


Port Distributions



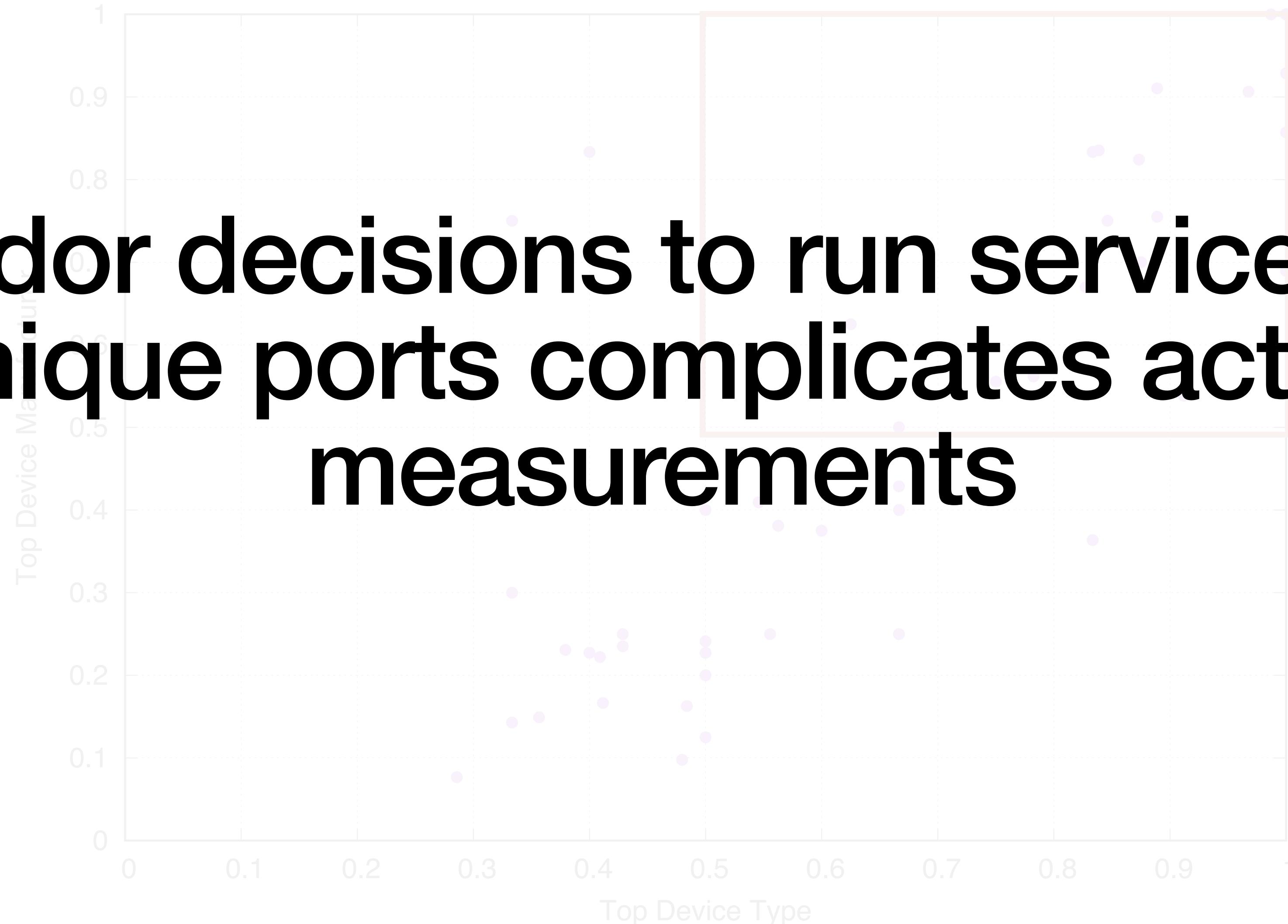
44% of ports were largely specific to a single manufacturer/device type

Port Distributions



Port Distributions

Vendor decisions to run services on unique ports complicates active measurements



Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Active Measurements through IoT Inspector

- Sent a SYN probe to a series of IoT specific ports informed by prior work and those used by Internet-scanning systems
- 73% of IoT devices in our network responded to at least one SYN probe
- Devices inside home networks support a host of active services, many popular ones run HTTP servers for remote control

Protocol	% Devices Support
8008/HTTP	36%
8443/HTTPS	36%
80/HTTP	31%
443/HTTPS	17%
8080/HTTP	12%
1843/—	11%
1443/—	11%
22/SSH	8%
8060/—	6%

Active services on IoT devices

Comparing Active Internal and Passive Internal

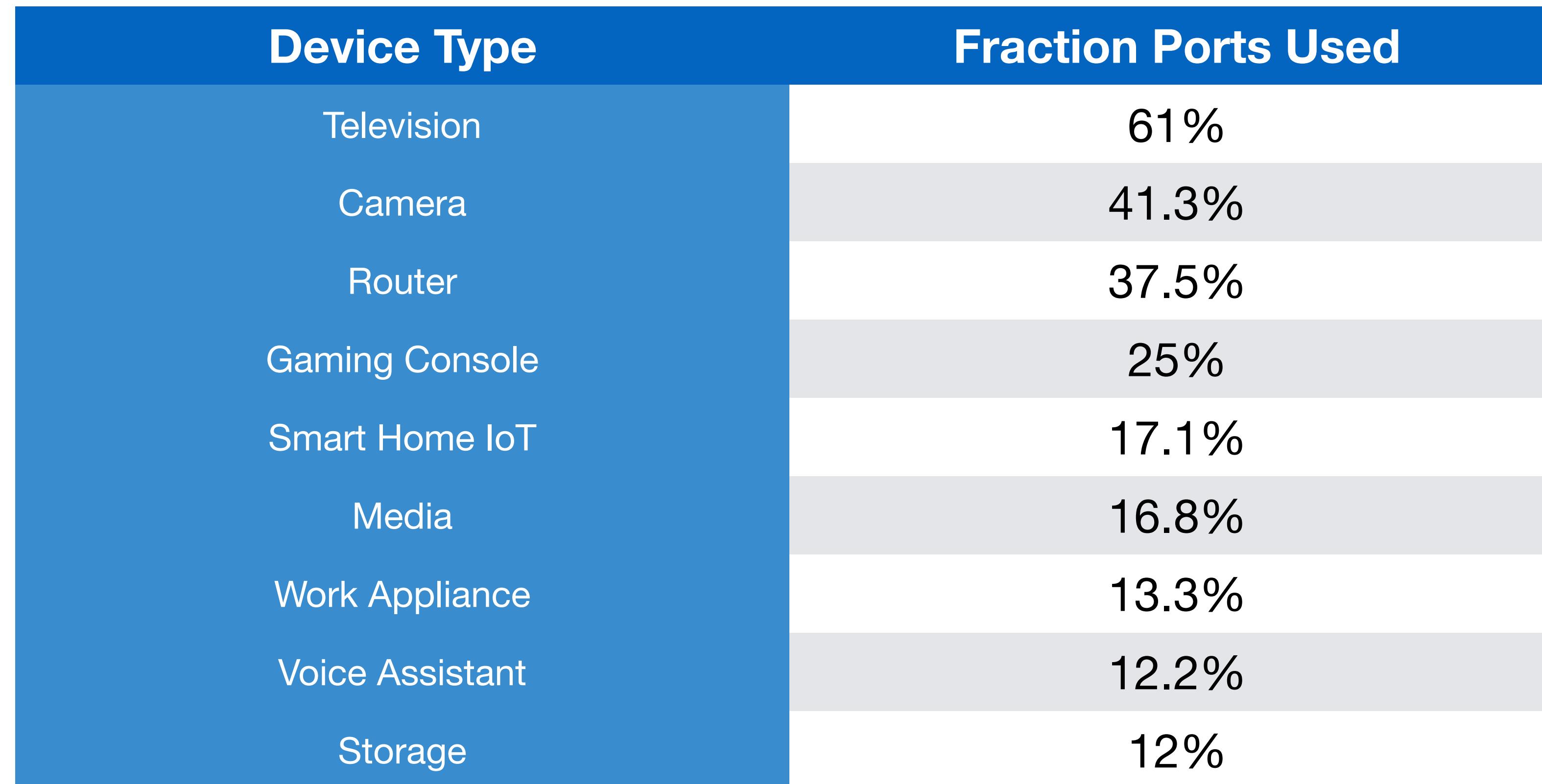
- Compared the protocols that were offered (through SYN scan) to the protocols we observed used by devices
- Devices use an average 19% of services offered during our measurement period

Comparing Active Internal and Passive Internal

- Compared the protocols that were offered (through SYN scan) to the protocols we observed used by devices
- Devices use an average 19% of services offered during our measurement period

Protocol	% Devices Unused	Can Explain?
22/SSH	100%	✗
9100/CUPS	100%	✓
8081/HTTP	100%	✗
111/rpcbind	100%	✗
8443/MQTT	97%	✓
23/Telnet	96%	✗

Comparing Active Internal and Passive Internal



Comparing Active Internal and Passive Internal

- Compared the protocols that were offered (through SYN scan) to the protocols we observed used by devices
- Devices use only a median 38% of services offered during our measurement period
- Many of these services are security critical (e.g., 23/Telnet, 111/rpcbind)

Device capabilities through active scanning are often much larger than device behavior through passive observation

Protocol	% Devices Unused	Can Explain?
22/SSH	100%	x
23/Telnet	100%	x
111/rpcbind	100%	x
8443/MQTT	97%	✓
23/Telnet	96%	x

Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Comparing Passive Internal to Passive External

- IoT Inspector captures traffic to the outside world as well as behavior on the local network
- Devices only use a small fraction of ports when communicating externally
- Primarily features communication over ports 53, 443, 80, all standard protocols to support DNS, HTTPS, and HTTP

Protocol	% Devices Communicated
53/UDP	69%
443/TCP	67%
80/TCP	43%
123/UDP	31%
443/UDP	12%
8883/TCP	6.4%

External Communication

Comparing Passive Internal to Passive External

Port	Protocol	Service	% Devices
8009	TCP	HTTP	12.5%
80	TCP	HTTP	9.9%
1400	TCP	HTTP	4.8%
10001	UDP	—	4.6%
8008	TCP	HTTP	4.4%
9000	TCP	—	2.9%
8060	TCP	HTTP	2.2%

Local Communication

Protocol	% Devices Communicated
53/UDP	69%
443/TCP	67%
80/TCP	43%
123/UDP	31%
443/UDP	12%
8883/TCP	6.4%

External Communication



Comparing Passive Internal to Passive External

Device Type	Fraction Observed Externally
Media	6%
Work Appliance	12.5%
Television	22%
Voice Assistant	27%
Smart Home IoT	35%
Storage	42%
Camera	75%

Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Comparing Active Internal to Passive External

- Devices inside home networks support a host of active services
- We *expect* the behavior of devices to the outside world to be different from the services offered inside networks
- We find no correlation between the services offered from active internal and passive external

Protocol	% Devices Support
8008/HTTP	36%
8443/HTTPS	36%
80/HTTP	31%
443/HTTPS	17%
8080/HTTP	12%
1843/—	11%
1443/—	11%
22/SSH	8%
8060/—	0%

Active services on IoT devices

Comparing Passive Internal to Passive External

Device Type	Fraction Observed Externally
Smart Home IoT	35%
Camera	75%
Television	22%
Work Appliance	12.5%
Storage	42%

External device behavior does not match internal device behavior or capabilities

Thesis Outline

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Comparing Active External to Passive Behavior

- Internal and external device behavior cannot be observed from active probing on the outside
 - At best, can attribute behavior to an externally facing router, but unknown if the router is producing the traffic
 - Recent research from Alrawi et. al suggests using a passive external fingerprint collected from homes (e.g., DNS traces) to identify IoT devices on the network, but this too cannot be observed through an active external probe

Recap

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Recap

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Recap

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Recap

	Active Measurement	Passive Measurement
Internal Vantage Point	All Things Considered IoT Inspector	IoT Inspector
External Vantage Point	Understanding the Mirai Botnet	IoT Inspector

Principles for Measuring IoT

- An internal vantage point provides access to finer-grained data about network behaviors and capabilities compared to external vantage points
- IoT Devices often exhibit different behaviors and capabilities, requiring both passive and active measurement to properly quantify

Principles for Measuring IoT

- An internal vantage point provides access to finer-grained data about network behaviors and capabilities compared to external vantage points
- IoT Devices often exhibit different behaviors and capabilities, requiring both passive and active measurement to properly quantify

Differences in network services are best captured by a local network vantage point using active and passive techniques.

Lessons Learned and Future Directions

- Our results challenge current security assumptions about IoT devices and their behavior
- Homesnitch, Hestia, HoneyScope aim to improve local network security guarantees
 - Network behavior in practice is more complex than simple “hub/device” model
- Alrawi et. al, and Huang et. al primarily use external IoT network behavior to make claims about threat models: DNS, HTTP, UPnP, NTP
 - However, local network behavior shows us that there are far more ports, services, and protocols, many of which we could not identify
- Our results can help inform future security systems to match what happens in practice

Big Thank You!



Nikita Borisov



Adam Bates



Gang Wang



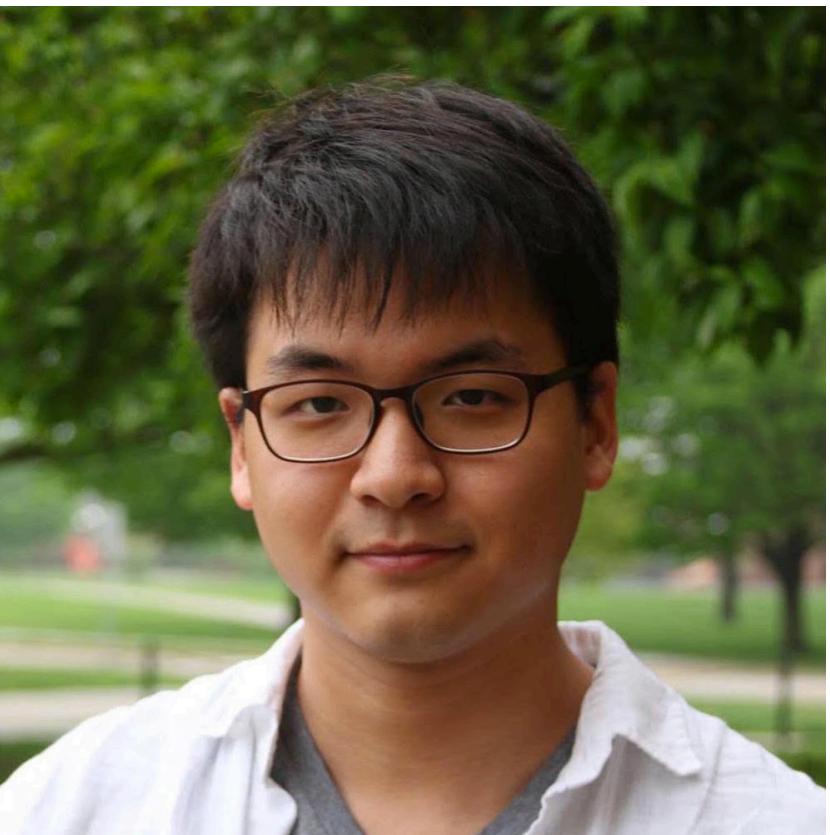
Zakir Durumeric

Would not have been possible without your guidance!

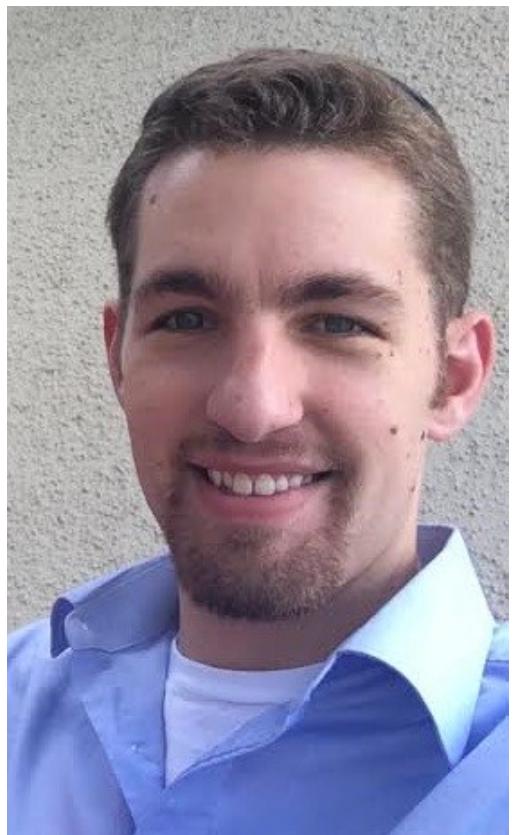
Big Thank You!



Zane Ma



Simon Kim



Paul Murley



Joshua Reynolds



Suyup Kim, Yi Zhou

Last But Not Least...



Lessons Learned and Future Directions

- Our results challenge current security assumptions about IoT devices and their behavior
- Homesnitch, Hestia, HoneyScope aim to improve local network security guarantees
 - Network behavior in practice is more complex than simple “hub/device” model
- Alrawi et. al, and Huang et. al primarily use external IoT network behavior to make claims about threat models: DNS, HTTP, UPnP, NTP
 - However, local network behavior shows us that there are far more ports, services, and protocols, many of which we could not identify
- Our results can help inform future security systems to match what happens in practice

Questions?

