

# Watching IoTs that watch us

Danny Y. Huang  
Assistant Professor



Collaborators: [Gunes Acar](#), Noah Apthorpe, [Frank Li](#), Hooman Mohajeri Moghaddam, Arunesh Mathur, Ben Burgess, Prateek Mittal, Arvind Narayanan, Edward Felten, Nick Feamster

# Video: I'm watching my TV while it is watching me

**ROKU**



# Video: I'm watching my TV while it is watching me

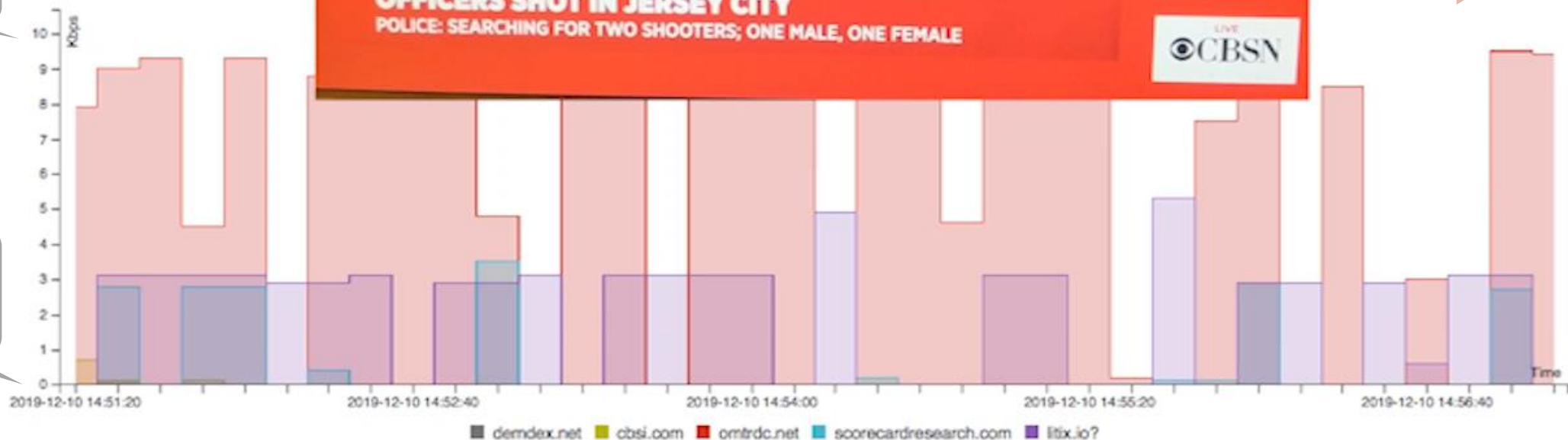
**ROKU®**



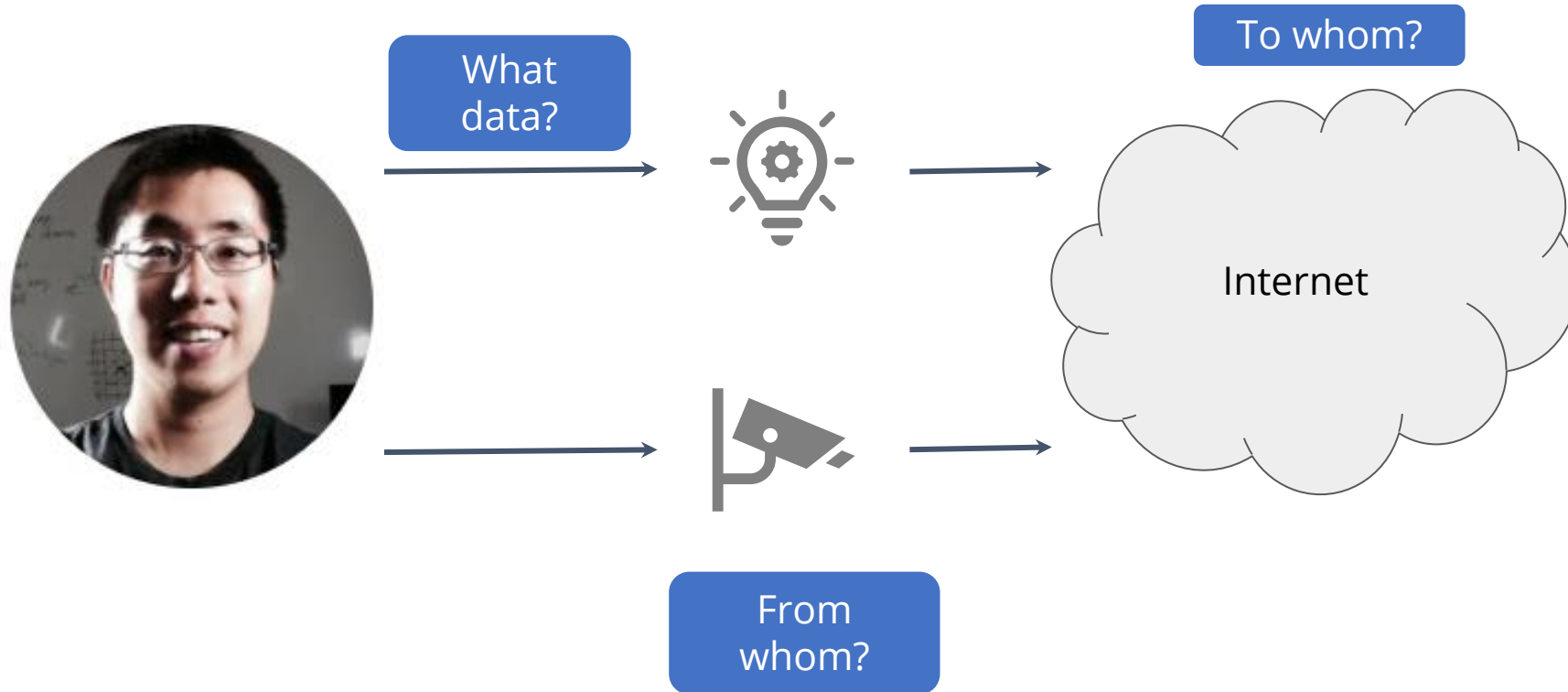
**Adobe®**  
Adobe  
Marketing  
Cloud

Kbps

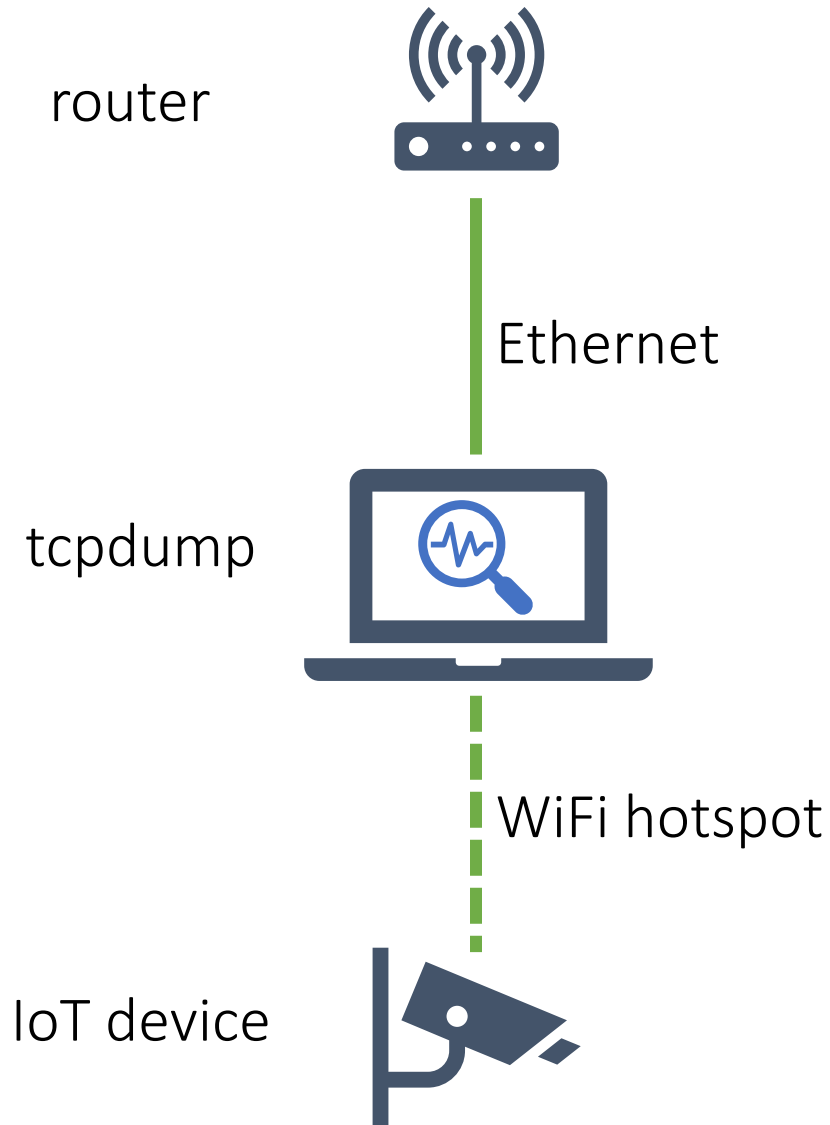
Time  
(10x)



# Many consumers are concerned about IoT security and privacy



# Analyzing devices' operational network traffic in lab



Are connections correctly encrypted?

Which Internet service is device talking to?

What data is being sent by device?

Google



amazon

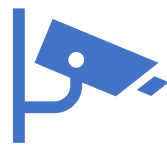
**alhua**  
TECHNOLOGY

**SAMSUNG**

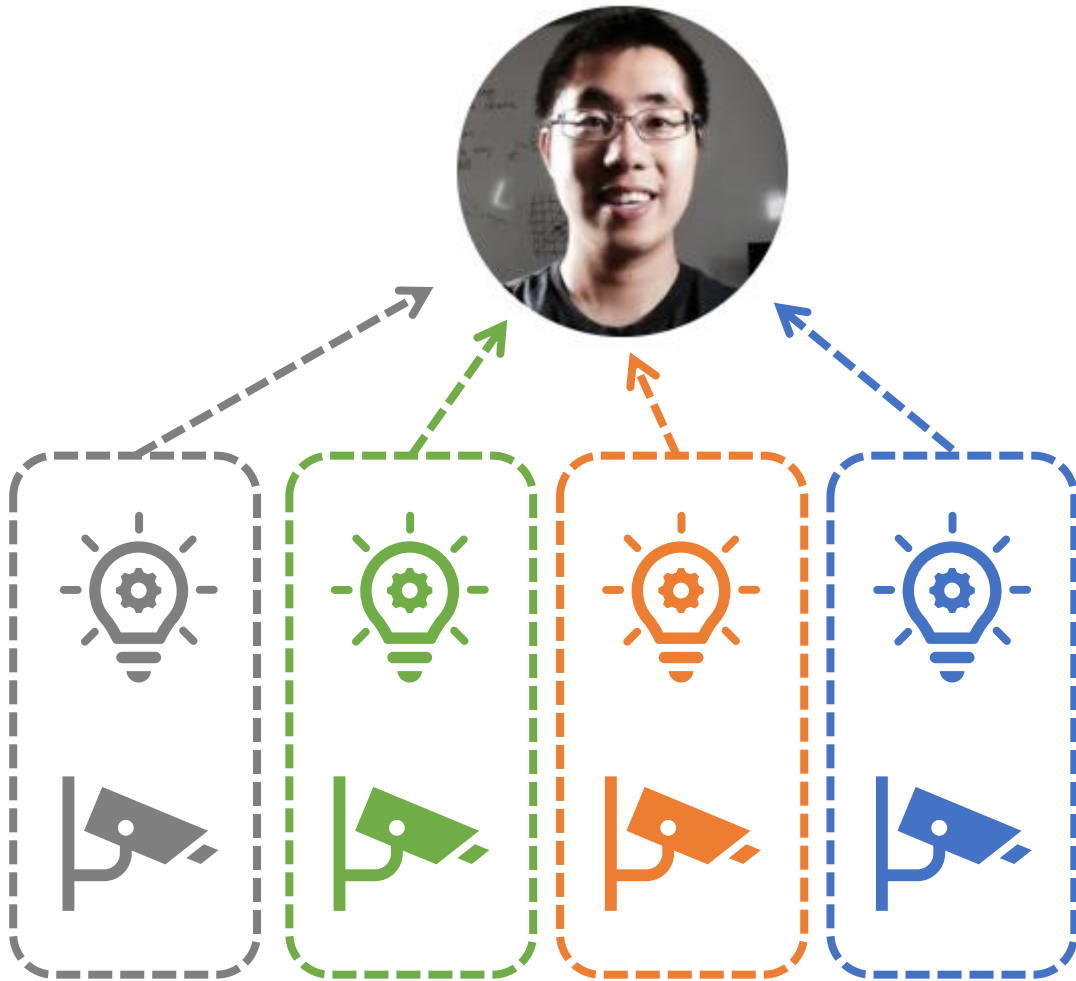
**HIKVISION**



# Difficult to study IoT security and privacy at scale



# Crowdsource IoT traffic at scale



**usable** tool that offers insight on IoT security and privacy

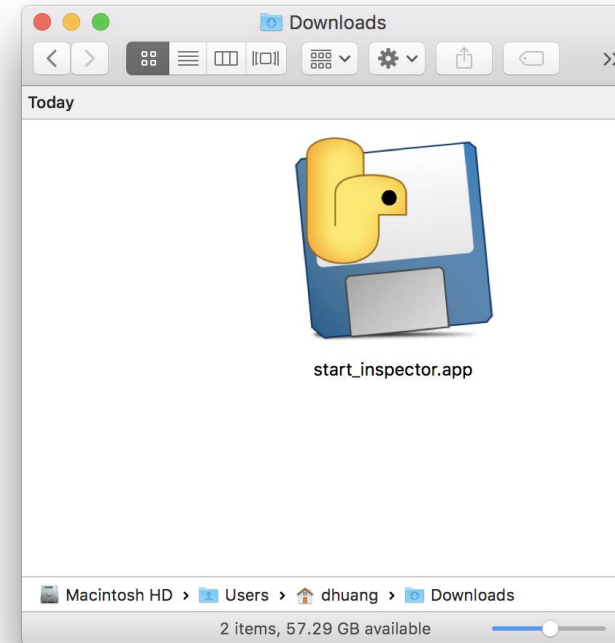
collect **anonymized** network traffic data

develop open-source tool  
**IoT Inspector**

# Downloading and running IoT Inspector



<https://iotinspector.org>





# Downloading and running IoT Inspector

The screenshot shows the Princeton IoT Inspector web interface. The browser address bar displays `https://inspector.cs.princeton.edu/dashboard`. The page title is "Princeton IoT Inspector" with a "Settings" link. A "Persistent Mode" indicator is in the top right.

## My Devices

Here are the devices on your network, automatically updated every 10 seconds.

You don't see your device(s) below? Try to [rescan network](#), or read [this FAQ](#).

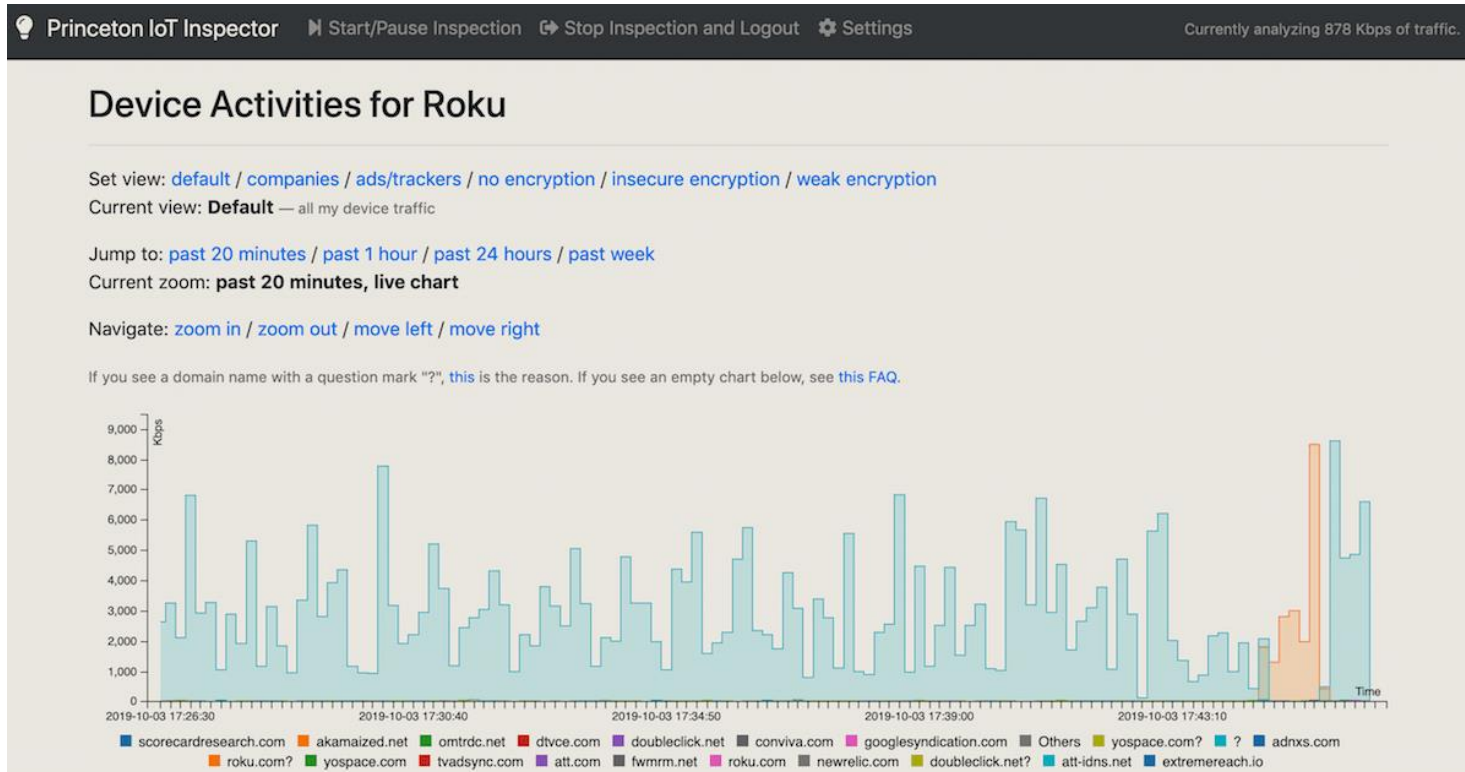
All your monitored devices are shown as "No Data"? Read [this FAQ](#).

[monitor all devices](#) | [un-monitor all devices](#)

Show  entries Search:

Monitored	Device	Last Updated
<input checked="" type="checkbox"/>	<b>Wemo Switch</b> IP Address: 10.6.6.13 / MAC Address: 14:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago
<input checked="" type="checkbox"/>	<b>D-Link Camera</b> IP Address: 10.6.6.14 / MAC Address: B0:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago
<input checked="" type="checkbox"/>	<b>Amcrest Camera</b> IP Address: 10.6.6.15 / MAC Address: 4C:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago
<input checked="" type="checkbox"/>	<b>Samsung Smart TV</b> IP Address: 10.6.6.19 / MAC Address: 28:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago

# Insights from an independent user



Ira Flatow  
Host of Science Friday

“Here is what the **Princeton IoT Inspector** tracked in a 20 minute time span on Ira’s Roku.”

(October 4, 2019)

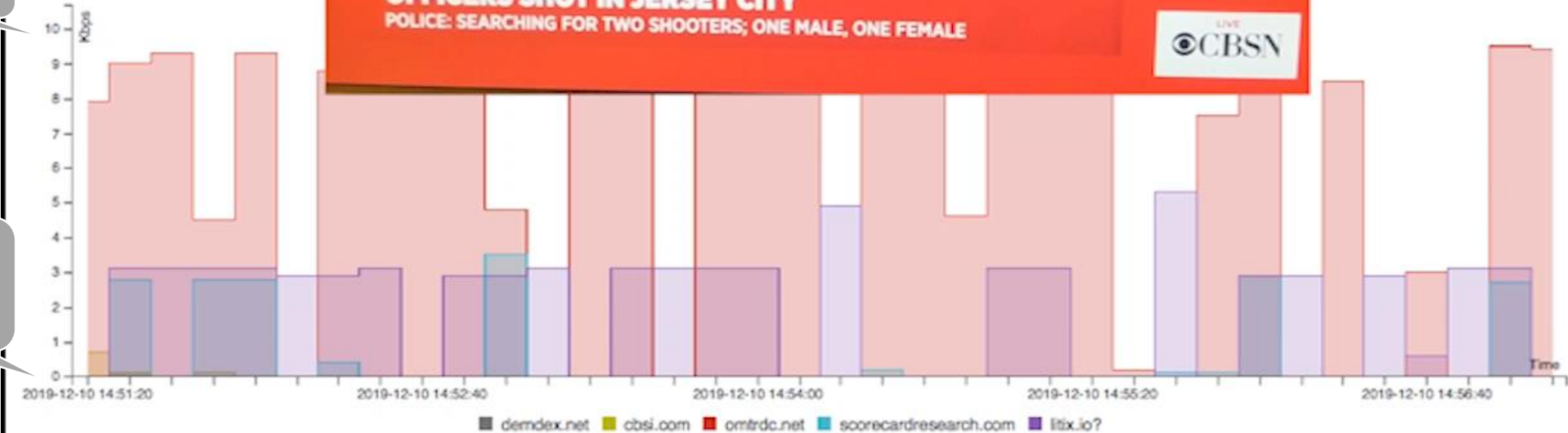
*Insight* — Ira’s Roku TV constantly communicated with advertising and tracking services

# Video: IoT Inspector showing network activities of Roku TV

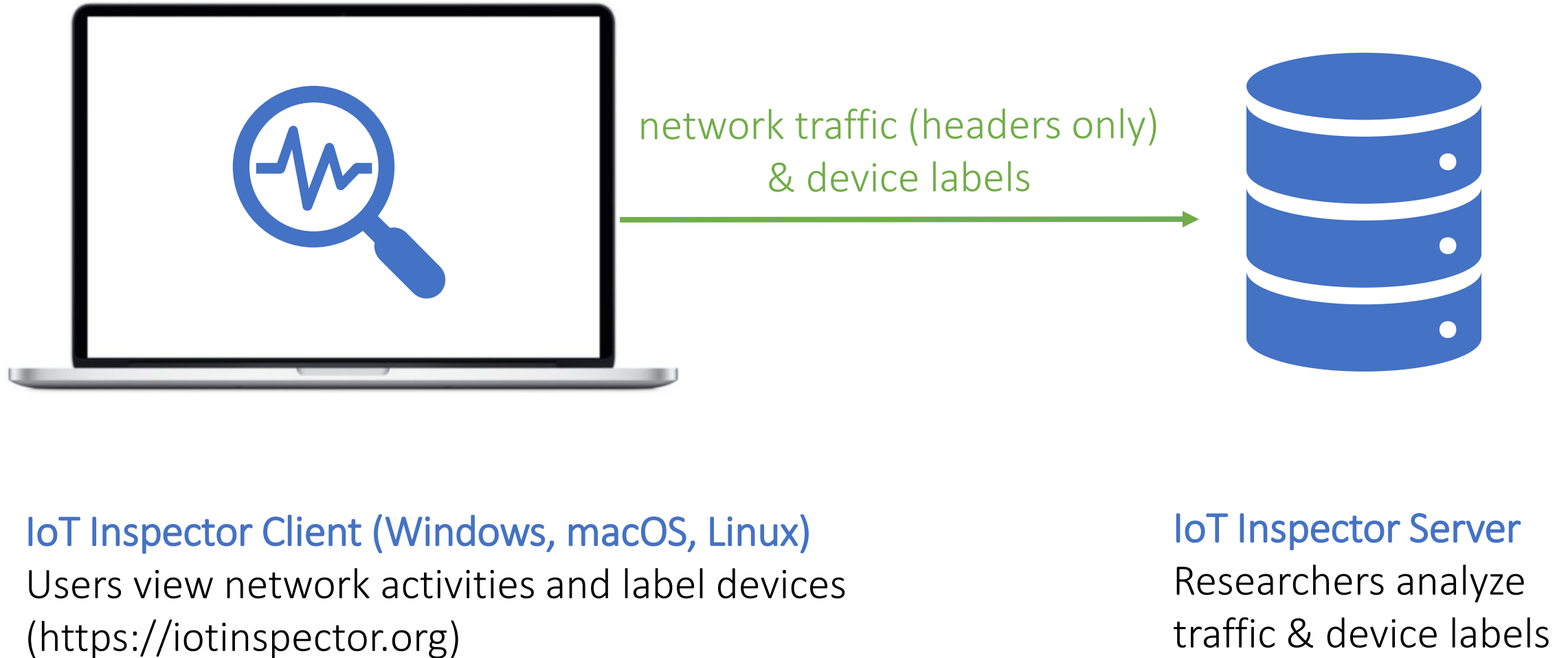


Kbps

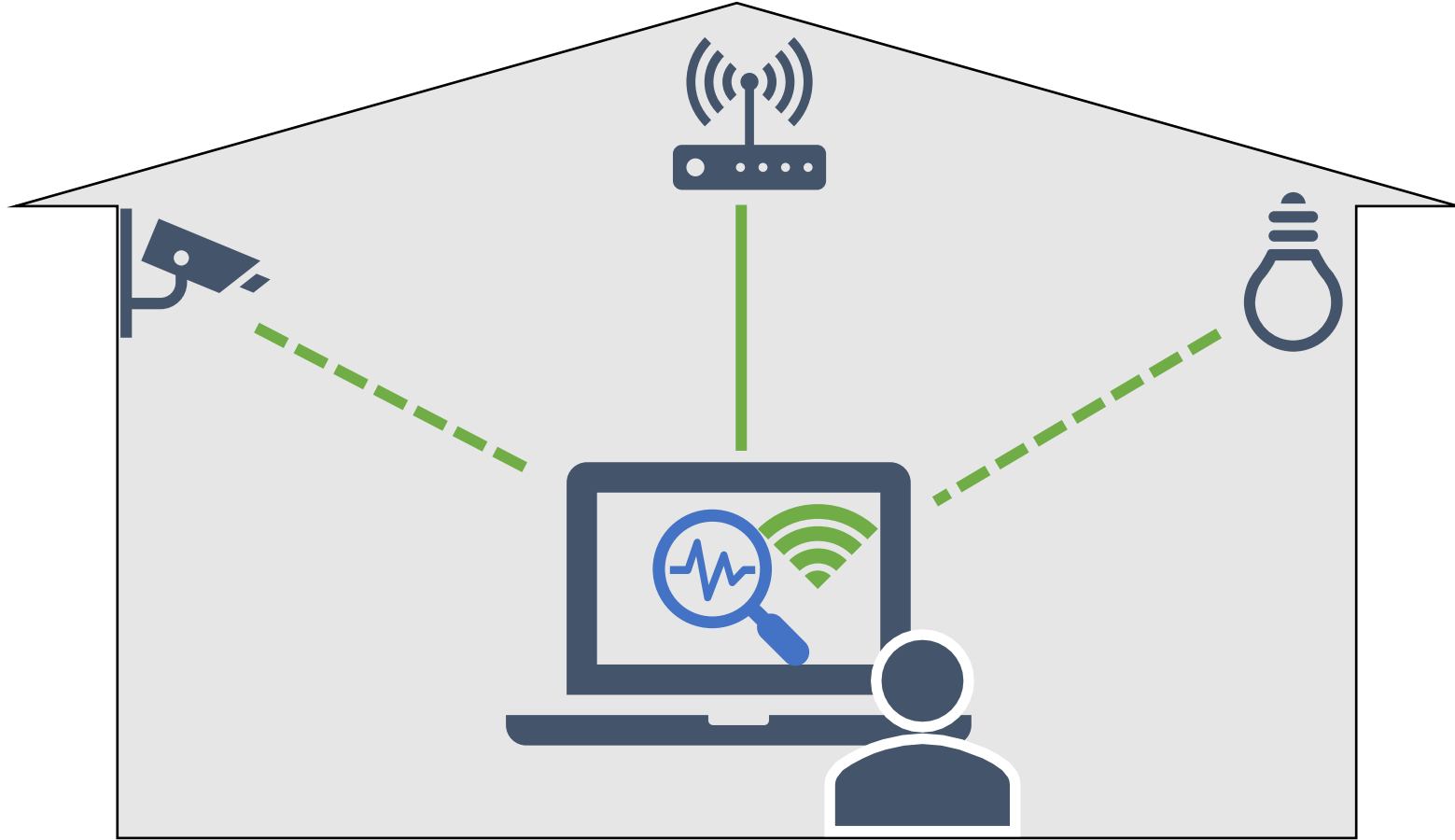
Time (10x)



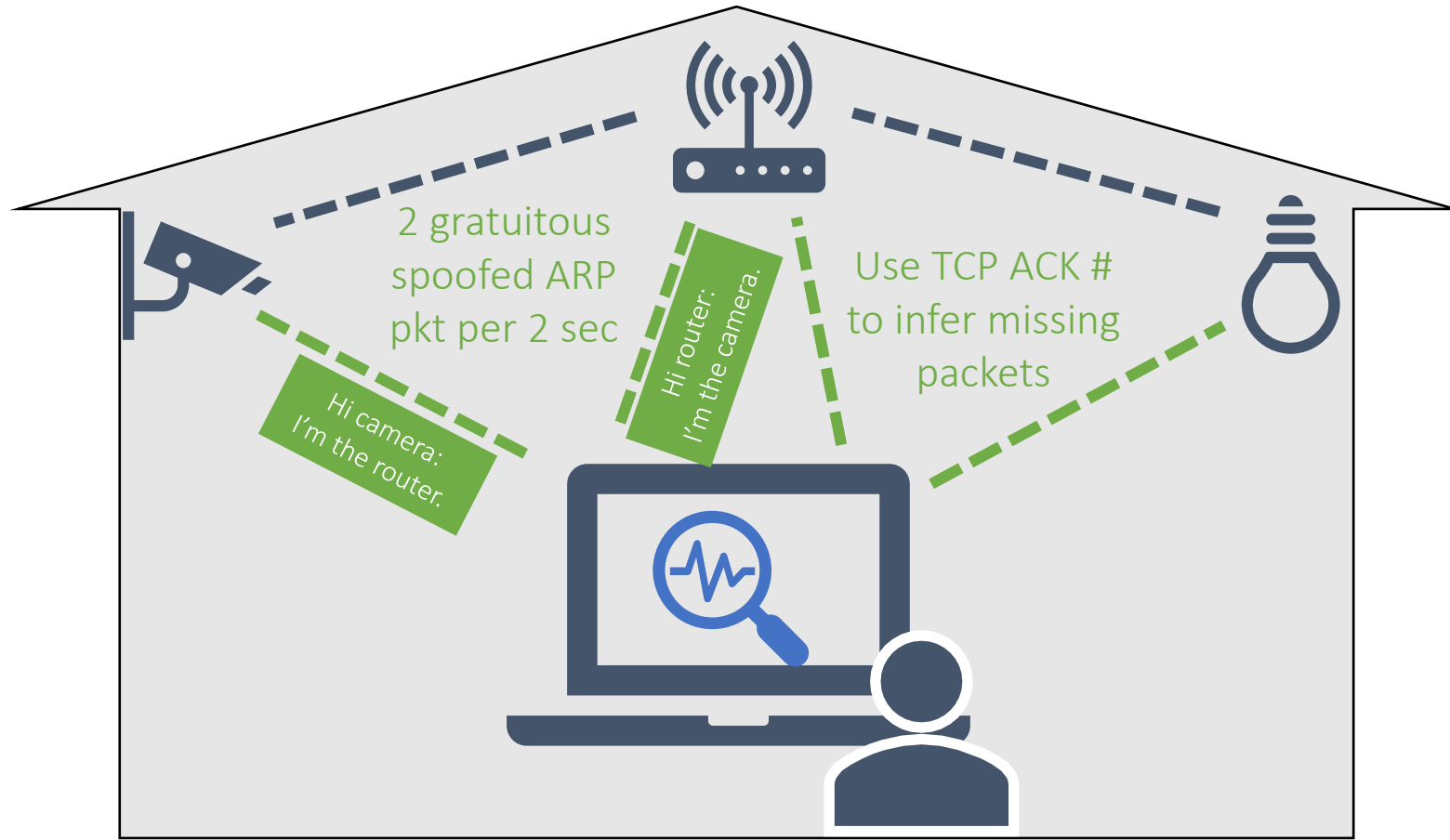
# IoT Inspector: usable system to crowdsource IoT network traffic at scale



# Strawman: capturing network traffic by creating a WiFi hotspot



# Our technique: passive traffic analysis via ARP spoofing



# Contributions of IoT Inspector



## Tool

5,400+ anonymous users since April '19  
Still gaining users and collecting data



## Dataset

54,000+ Internet-connected devices  
12,000+ device labels  
10+ organizations requesting data access



## Insight

Security: Non-encryption, exposed local services  
Privacy: Tracking on smart TVs

### Users



The Washington Post  
The New York Times



### Collaborators





# Insight: Found potential MITM vulnerabilities



36% of devices\* communicate over HTTP (port 80)

Covering 69 out of 81 vendors

Examples: Lutron, iHome, Amazon, Roku



10% of devices\* that used SSL/TLS used outdated versions (e.g., SSL 3.0 and TLS 1.0)

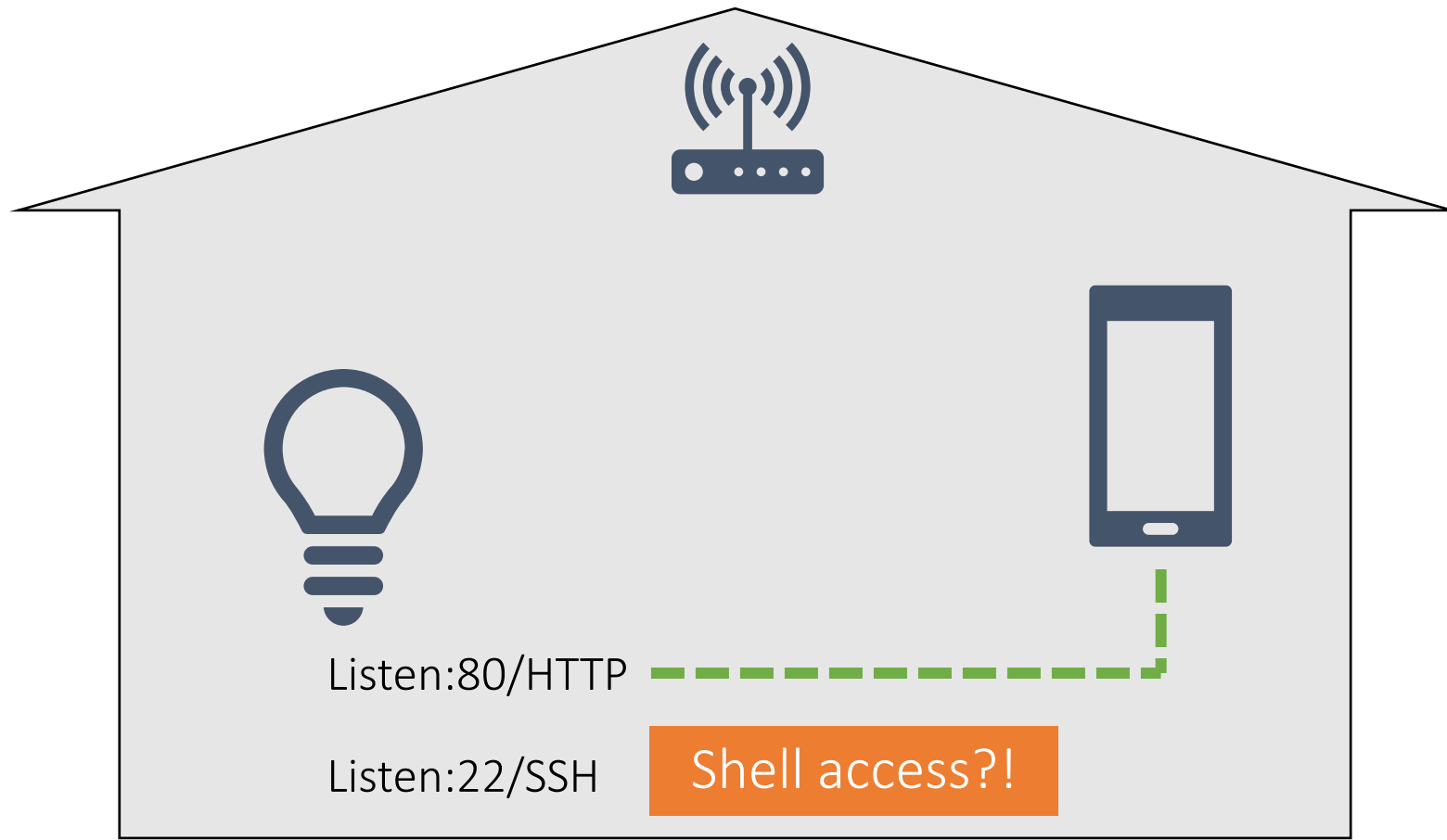
Covering 26 vendors

Examples: Amazon, Vizio, Samsung

On-path attacker  
can see your traffic  
(i.e., man-in-the-middle attack)

\* weighted by the number of devices for each vendor

# Insight: Some local ports are unused and could be exploited



# Insight: Some local ports are unused and could be exploited

Top Local Ports	% devices	
8008/HTTP		
8443/MQTT		
80/HTTP		
22/SSH		
139/SMB		

# Insight: Some local ports are unused and could be exploited

Top Local Ports	% devices	
8008/HTTP	36%	
8443/MQTT	36%	
80/HTTP	31%	
22/SSH	8%	
139/SMB	6%	

# Insight: Some local ports are unused and could be exploited

Top Local Ports	% devices	Top Unused Local Ports	% unused
8008/HTTP	36%	22/SSH	100%
8443/MQTT	36%	8081/HTTP	100%
80/HTTP	31%	23/Telnet	96%
22/SSH	8%	443/HTTPS	93%
139/SMB	6%	139/SMB	92%

Potential security vulnerability

# Insight: Tracking on smart TVs

417 smart TVs in the dataset

22% of registered domains contacted by these smart TVs are advertising/tracking services, based on Disconnect List



Most TVs talk to what advertising/tracking companies?

A: Google

B: Amazon

C: Facebook

D: Others

# Insight: Tracking on smart TVs

417 smart TVs in the dataset

22% of registered domains contacted by these smart TVs  
are advertising/tracking services, based on Disconnect List



doubleclick.net

34%

of smart TVs



scorecardresearch.com

14%

of smart TVs



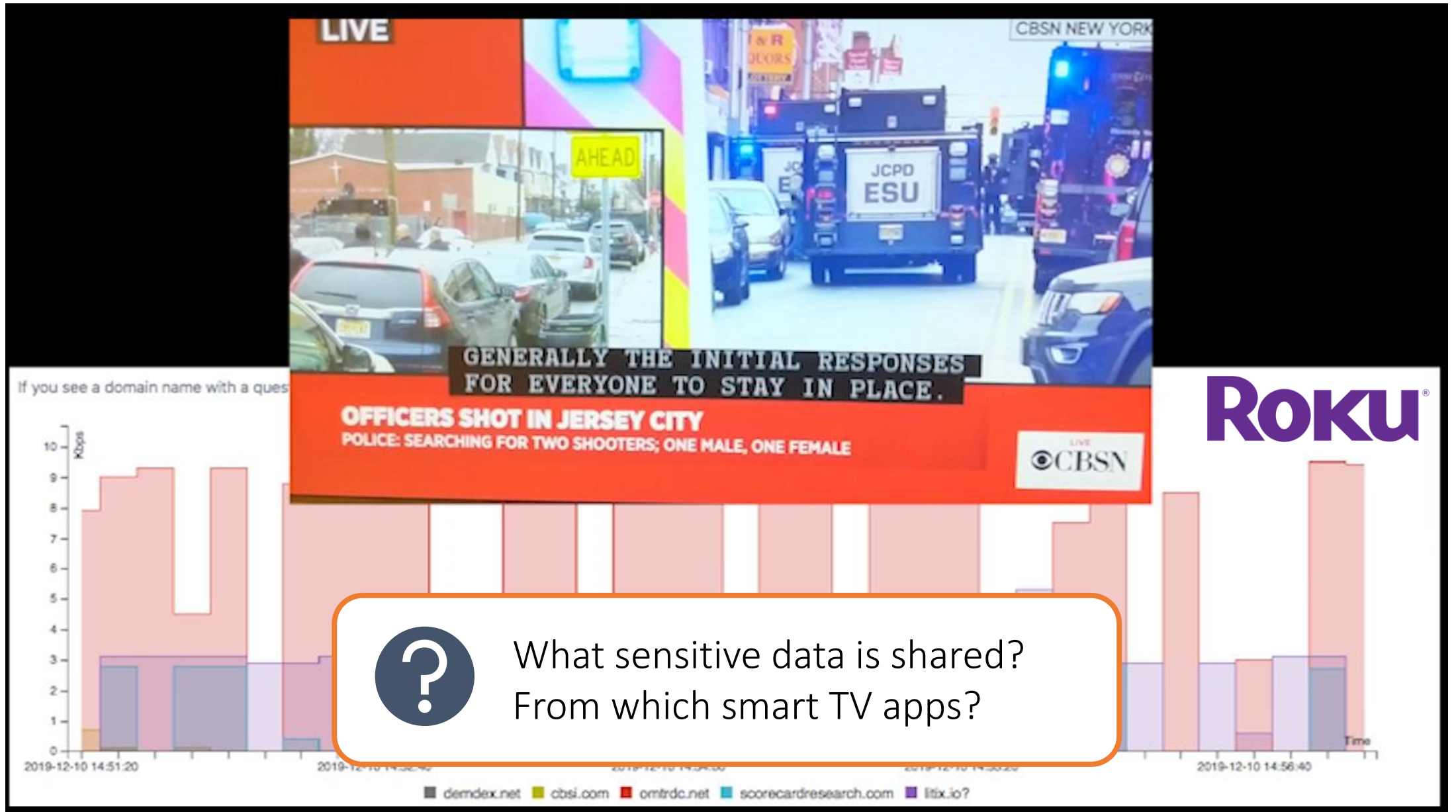
fwmrm.net

5%

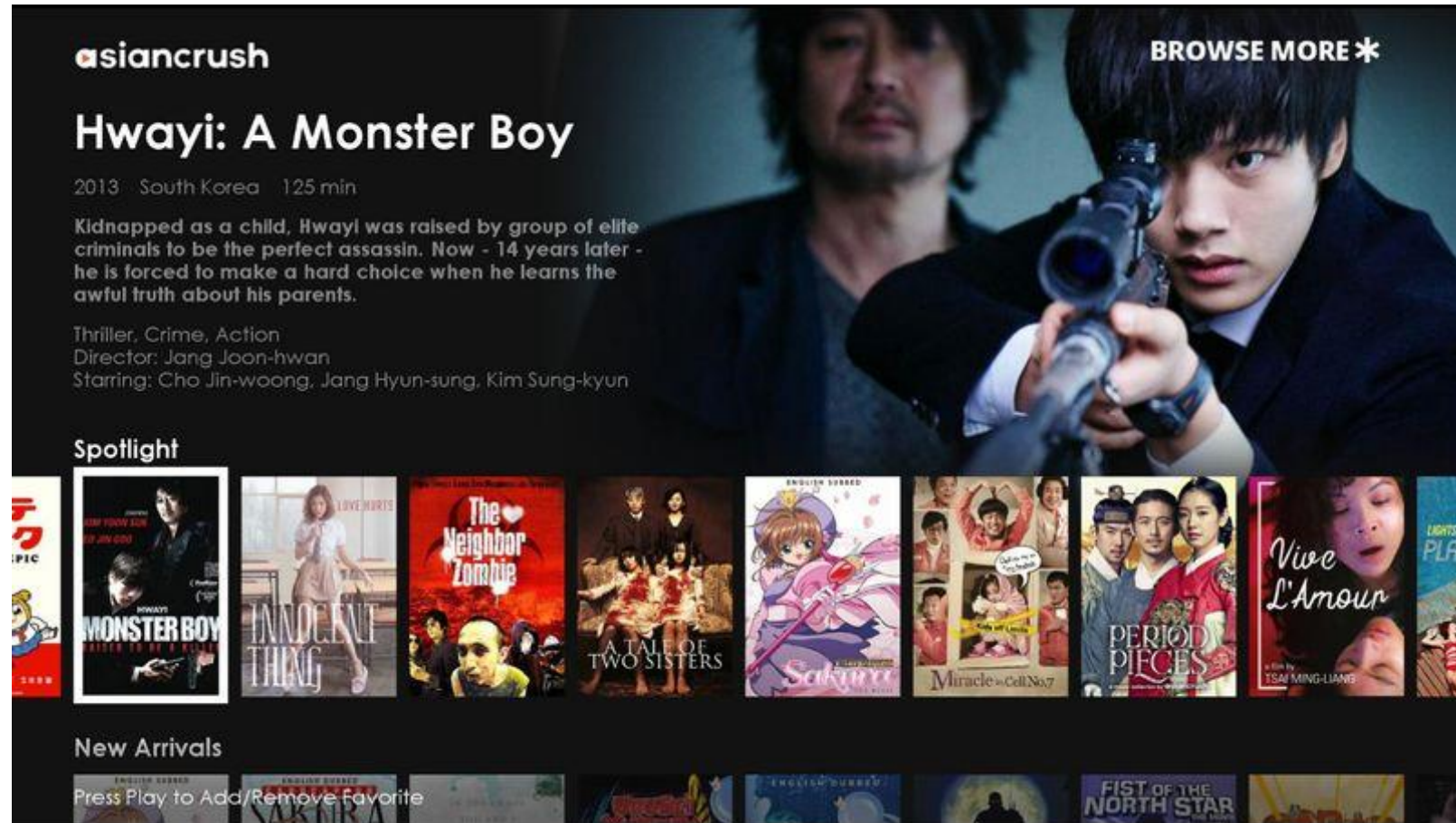
of smart TVs



# Limitation of IoT Inspector's dataset



# Challenges of analyzing smart TV traffic in lab



# Challenges of analyzing smart TV traffic in lab



**SPOTX**

# So%20Young%20%3A%20Never%20Gone

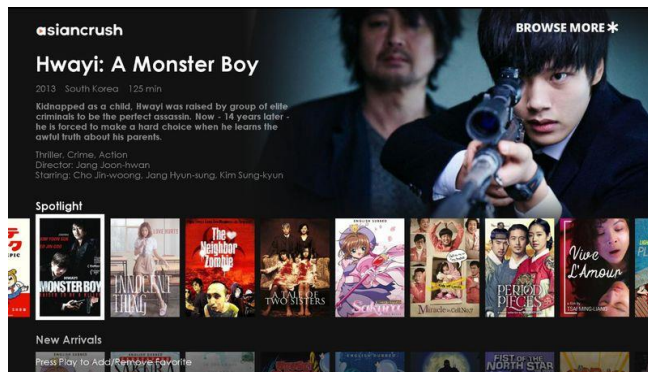
HTTP outbound to 192.35.249.124:80 (DNS: search.spotxchange.com) (channel name: asiancrush)

```
GET /vast/3.0/146141?VPI[]=MP4&VPI[]=ROKU&app[name]=asiancrush&app[domain]=asiancrush.com&
app[bundle]=com.dmr.asiancrush&player_width=1280&player_height=720&device[devicetype]=7&de
vice[make]=Roku&device[model]=Roku&device[ifa]=39fc6352-aede-53f6-b3e3-58bf562bd074&ip_add
r=128.112.139.195&cb=1557313464653&custom[movie_title]=So%20Young%20%3A%20Never%20Gone&cu
stom[content_id]=3417&token[device_id]=39fc6352-aede-53f6-b3e3-58bf562bd074&token[connecti
on]=wifi&token[category_ID]=241&token[category_Title]=Romance&device[dnt]=0&max_bitrate=70
00 HTTP/1.1
```

Host: search.spotxchange.com

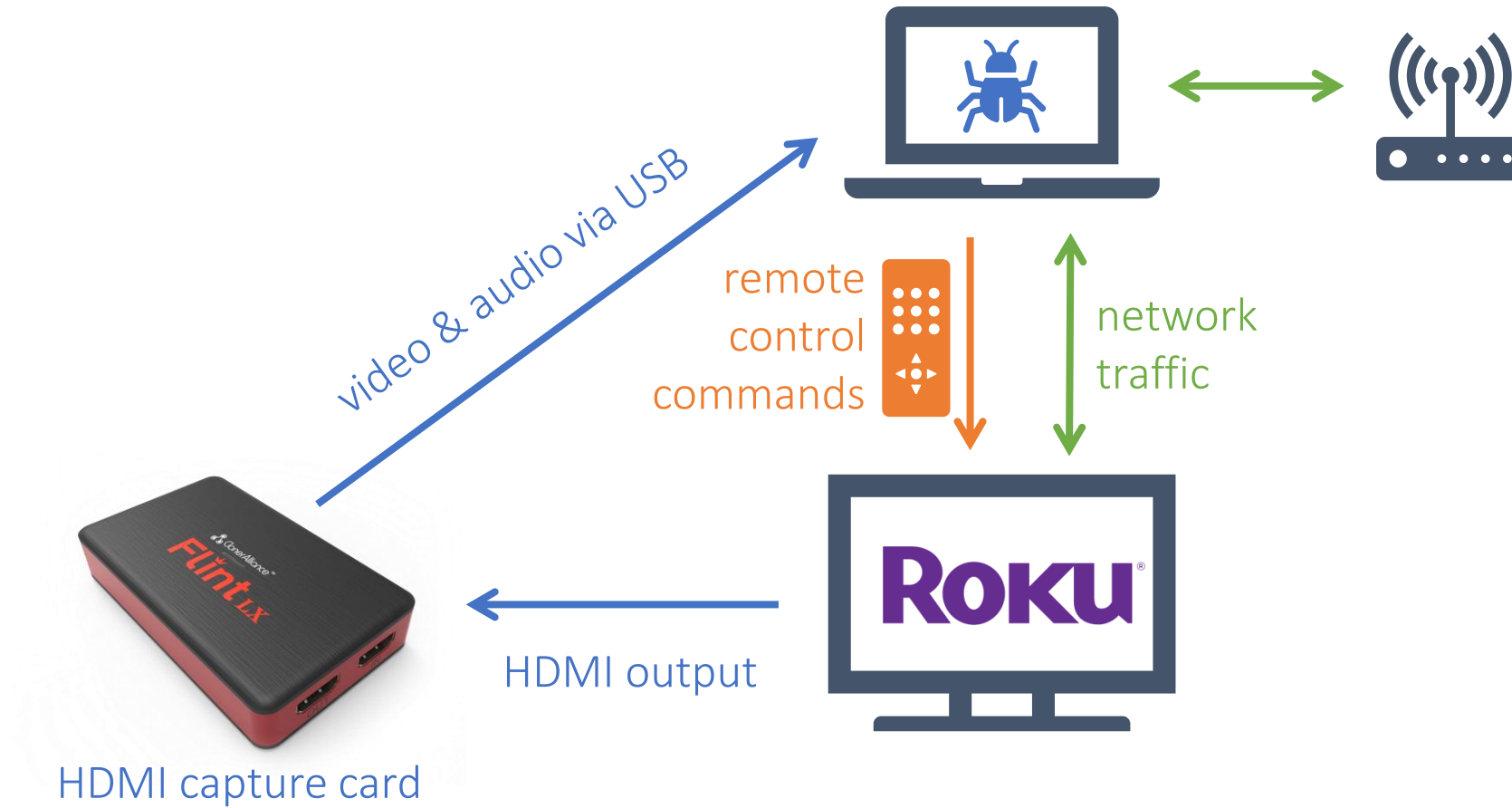
User-Agent: Roku/DVP-9.0 (519.00E04142A)

Accept: \*/\*



# How to analyze the traffic of TV apps at scale?



# Automating interactions with smart TVs



# Findings: sensitive data shared with ad/tracking services



<b>Roku®</b>	% apps	<b>amazon</b>	% apps
Ad ID			
App name			
Serial number			
Zip code			
City or state			

# Findings: sensitive data shared with ad/tracking services

	% apps		% apps
Ad ID	32%		
App name	20%		
Serial number	11%		
Zip code	1%		
City or state	1%		



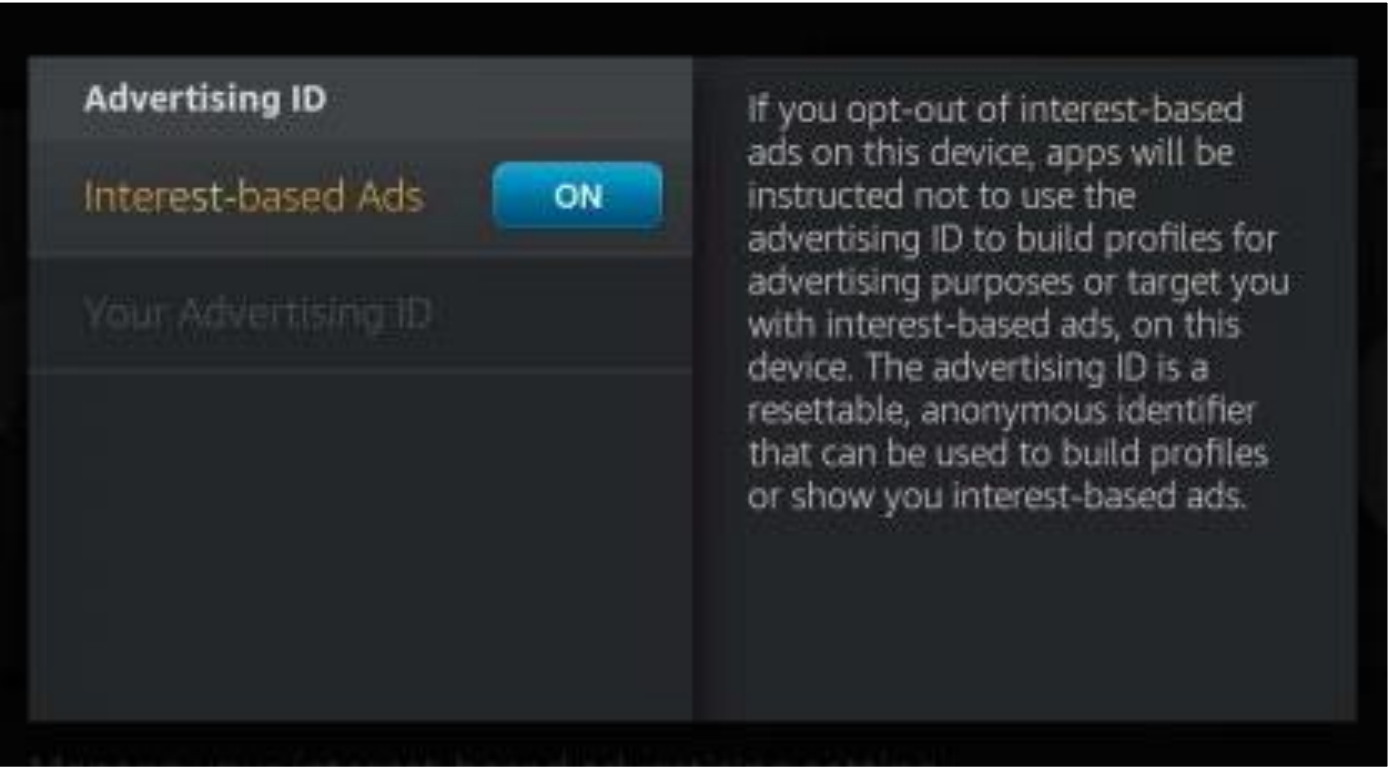
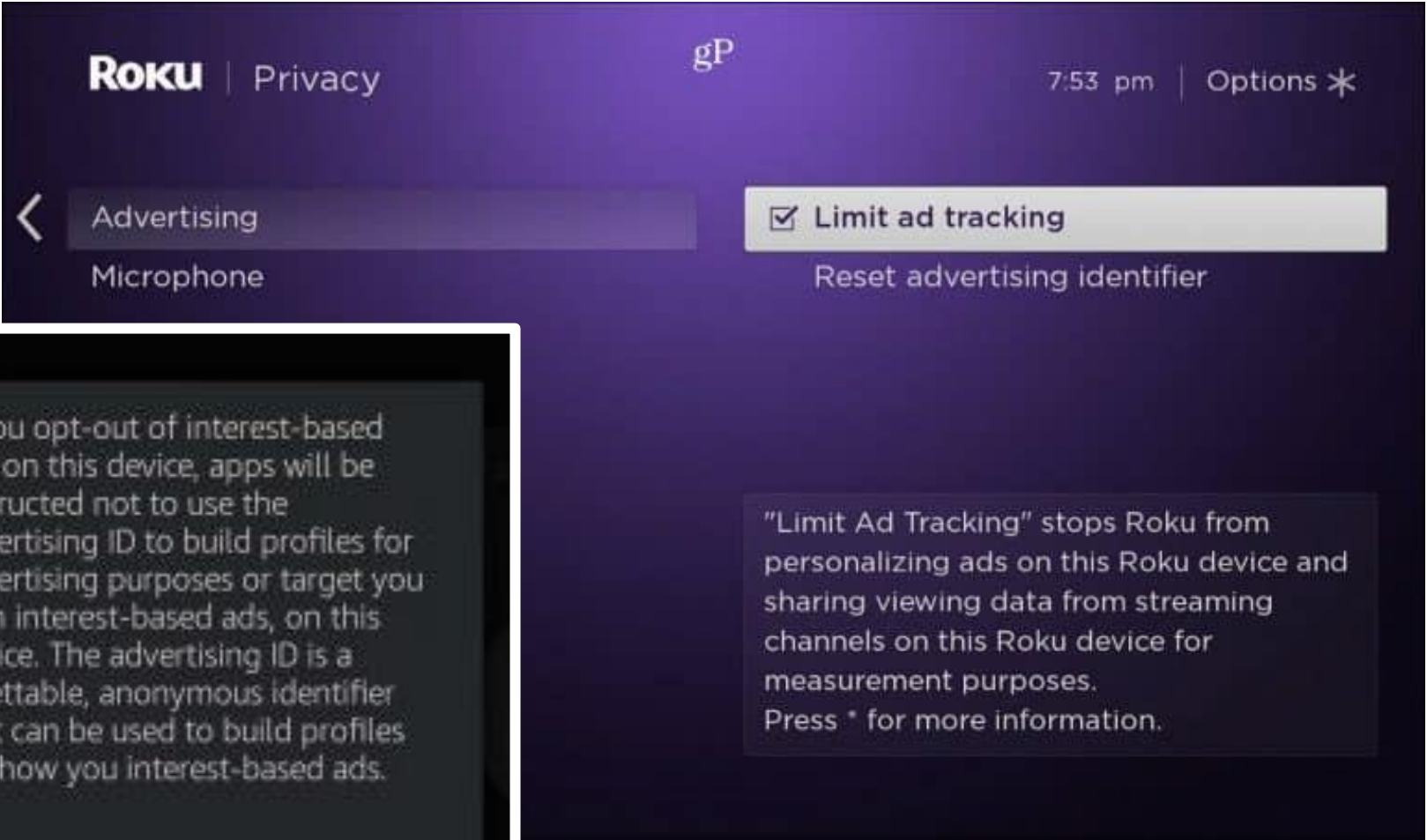
# Findings: sensitive data shared with ad/tracking services

	% apps		% apps
Ad ID	32%	Android ID	39%
App name	20%	Ad ID	22%
Serial number	11%	Serial number	10%
Zip code	1%	MAC address	5%
City or state	1%	WiFi SSID	2%





# Limited ad tracking (Roku) / No interest-based ads (Amazon)



# Poll: What happens when you disable ad tracking?

	<b>Roku®</b>	% apps	<b>amazon</b>	% apps
A	Ad ID	32%	Android ID	39%
B	App name	20%	Ad ID	22%
C	Serial number	11%	Serial number	10%
	Zip code	1%	MAC address	5%
	City or state	1%	WiFi SSID	2%
D	All zero!			

Finding: 0 apps sent Ad ID under “limited tracking”

<b>Roku®</b>	% apps	<b>amazon</b>	% apps
Ad ID	32%	Android ID	39%
App name	20%	Ad ID	22%
Serial number	11%	Serial number	10%
Zip code	1%	MAC address	5%
City or state	1%	WiFi SSID	2%

# Privacy for children?



**FEDERAL TRADE  
COMMISSION**

September 4, 2019

## Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law

**FTC, New York Attorney General allege YouTube channels collected kids' personal information without parental consent**

The "FTC and New York Attorney General allege that YouTube violated the COPPA Rule by collecting personal information—in the form of **persistent identifiers** that are used to track users across the Internet—from viewers of **child-directed apps**, without first notifying parents and getting their **consent**."

# Privacy for children?



**FEDERAL TRADE  
COMMISSION**

September 4, 2019

## Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law



**FTC, New York Attorney General allege YouTube channels collected kids' personal  
information without parental consent**

The “FTC and New York Attorney General allege that YouTube violated the COPPA Rule by collecting personal information—in the form of **persistent identifiers** that are used to track users across the Internet—from viewers of **child-directed apps**, **without** first notifying parents and getting their **consent**.”

# Findings from smart TV study: privacy leaks in child-directed apps

	Roku	amazon
Number of apps	1,882	1,183
Number of child-directed apps	470	220

# Findings from smart TV study: privacy leaks in child-directed apps

		
Number of apps	1,882	1,183
Number of child-directed apps	470	220
Number of child-directed apps that leaked persistent IDs	34	23



# Examples of persistent IDs in child-directed apps



PBS KIDS Video

Oct 16, 2012 | by PBS KIDS

★★★★☆ ~ 4,547

App

FREE

Available instantly on compatible devices.

Leaked  
Android ID



Fun with Roblox by HappyKids.tv

Jan 4, 2019

★★★★☆ ~ 88

App

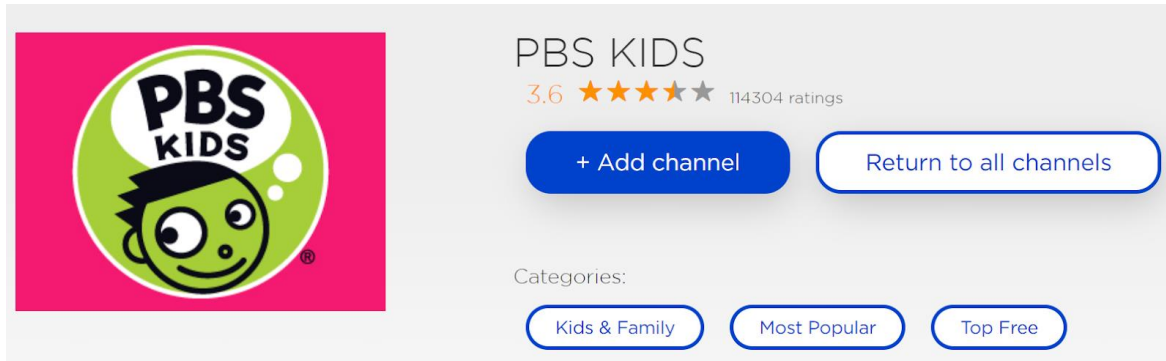
FREE

Available instantly on compatible devices.

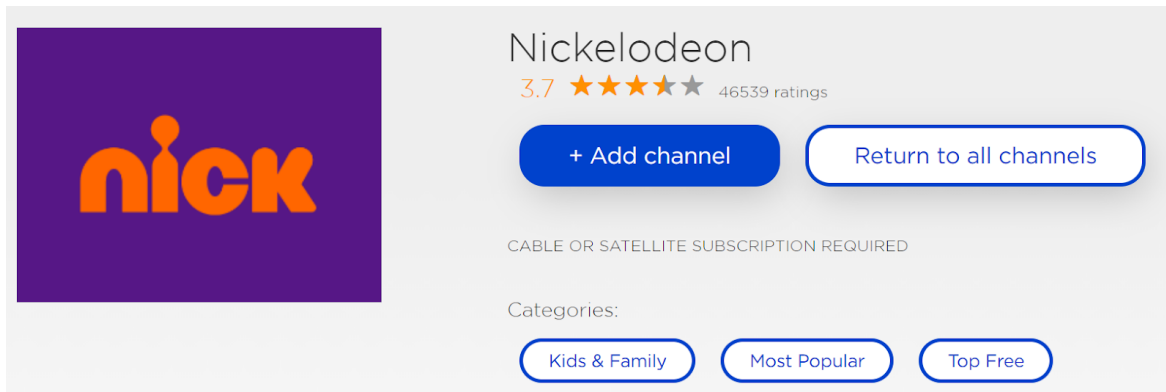
Leaked  
Android ID  
Serial Number

# Examples of persistent IDs in child-directed apps

**ROKU**



Leaked  
Ad ID  
Serial Number



Leaked  
Ad ID  
Serial Number

# Summary of current work



## Tool

5,400+ anonymous users since April '19  
Still gaining users and collecting data



## Dataset

54,000+ Internet-connected devices  
12,000+ device labels  
10+ organizations requesting data access



## Insight

Security: Non-encryption, exposed local services  
Privacy: Tracking on smart TVs

### Users



The Washington Post  
The New York Times



### Collaborators



# Next steps: Yelp for IoT devices



## Yelp for IoT devices

- Transparency for consumers
- Cybersecurity insurance?
- Minimal security standards?

What properties do consumers care about?

Sharing data with community

# Next steps: IoT supply chain analysis



?

==



**MOTHERBOARD**  
TECH BY VICE

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

As many predicted, hackers are starting to use your Internet of Things to launch cyberattacks.

By [Lorenzo Franceschi-Bicchieri](#)

September 29, 2016, 12:03pm [Share](#) [Tweet](#) [Snap](#)

### Understanding the Mirai Botnet

Manos Antonakakis<sup>°</sup> Tim April<sup>‡</sup> Michael Bailey<sup>†</sup> Matthew Bernhard<sup>°</sup> Elie Bursztein<sup>°</sup>  
Jaime Cochran<sup>▷</sup> Zakir Durumeric<sup>°</sup> J. Alex Halderman<sup>°</sup> Luca Invernizzi<sup>°</sup>  
Michalis Kallitsis<sup>§</sup> Deepak Kumar<sup>‡</sup> Chaz Lever<sup>°</sup> Zane Ma<sup>†\*</sup> Joshua Mason<sup>†</sup>  
Damian Menscher<sup>°</sup> Chad Seaman<sup>‡</sup> Nick Sullivan<sup>▷</sup> Kurt Thomas<sup>°</sup> Yi Zhou<sup>†</sup>

<sup>‡</sup>Akamai Technologies <sup>▷</sup>Cloudflare <sup>°</sup>Georgia Institute of Technology <sup>°</sup>Google  
<sup>§</sup>Merit Network <sup>†</sup>University of Illinois Urbana-Champaign <sup>°</sup>University of Michigan

## Who makes an IoT device?

- Original Equipment Manufacturer (OEM)?
- Which devices share same config/code?  
Same TLS libraries?

Provides consumers with transparency

Ongoing work: see <https://iotinspector.org/projects>

## security

### Enterprise device identification

- Passive network traffic
- Active scans
- Hardware metadata (e.g., OUI)

### IoT firewall

- Limitations of commercial firewalls and MUD
- Develop automated rules
- Blocks per device or connection

## privacy

### Usability

- Privacy perception of users?
- How to raise user awareness?

### Third-party identification

- What companies do devices talk to?
- First-party? Third-party?

## misc

### Healthcare

- Can we infer human health status using network traffic from IoT devices?

### Education

- How to let students access IoT testbeds remotely and run experiments?