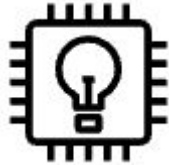
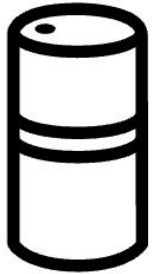


3 years of
crowdsourcing
smart home network traffic

Danny Y. Huang

Assistant Professor @ New York University

Smart home networks are getting increasingly complex



Security and privacy issues are often opaque to users and researchers



users

What's happening on my home network?
What's WireShark?



researchers

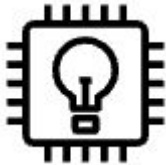
How to buy 1,000 IoT devices for my lab?
How to ask Company X for their IoT data?

IoT Inspector: an open-source monitoring tool for smart homes

Helping users visualize network activities of smart home devices



Download IoT Inspector on computer



IoT Inspector intercepts IoT traffic via ARP spoofing

Helping users visualize network activities of smart home devices



Providing researchers with a realistic large-scale dataset of IoT network traffic

63,000+

devices

with traffic metadata

since April 2019

6,400+

users



The Washington Post



Ongoing
research
papers

Smart TV privacy

IoT firewall

IoT TLS/PKI

IoT software supply chain security

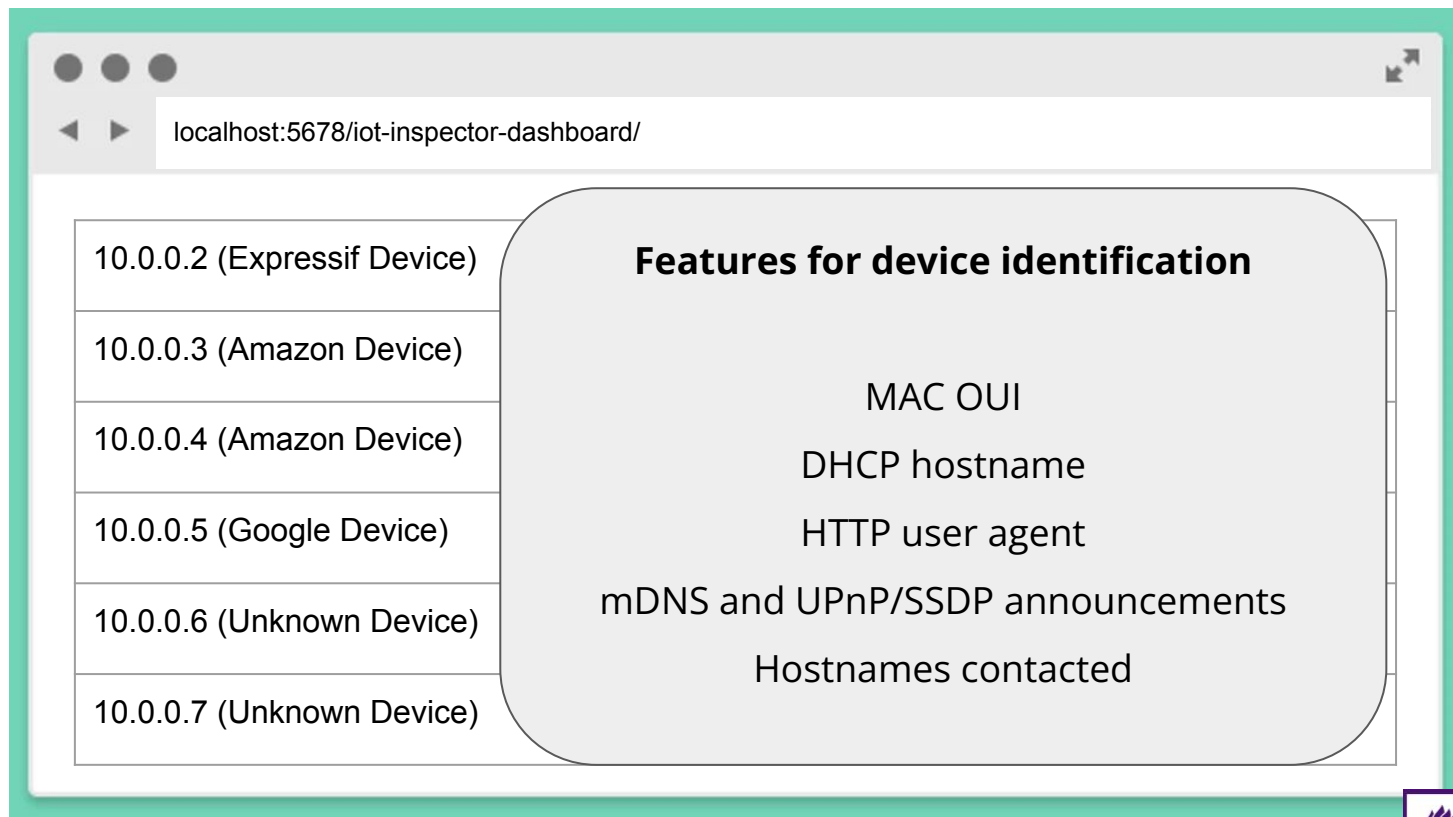
Smart home privacy and usability

“

What is this device?

Challenge 1: Identifying and labeling devices

Difficult for users to identify devices



The image shows a browser window with the address bar displaying `localhost:5678/iot-inspector-dashboard/`. On the left, a table lists several IP addresses and their associated device names. A large, rounded rectangular callout box is overlaid on the right side of the table, titled "Features for device identification".

10.0.0.2 (Expressif Device)
10.0.0.3 (Amazon Device)
10.0.0.4 (Amazon Device)
10.0.0.5 (Google Device)
10.0.0.6 (Unknown Device)
10.0.0.7 (Unknown Device)

Features for device identification

- MAC OUI
- DHCP hostname
- HTTP user agent
- mDNS and UPnP/SSDP announcements
- Hostnames contacted

Crowdsourced labels can be messy

Missing labels

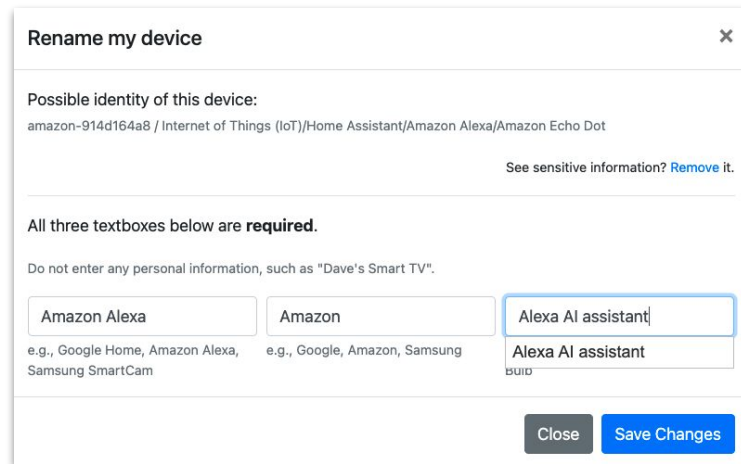
47% of users labeled at least one device
Users labeled 25% of devices

Inconsistent labels

Dropdown list + free text
"Amazon Echo" vs "Amazon Alexa"

Wrong labels

A smart fan that communicated with
hundreds of advertising services?



Rename my device ✕

Possible identity of this device:
amazon-914d164a8 / Internet of Things (IoT)/Home Assistant/Amazon Alexa/Amazon Echo Dot

[See sensitive information? Remove it.](#)

All three textboxes below are **required**.

Do not enter any personal information, such as "Dave's Smart TV".

Amazon Alexa	Amazon	Alexa AI assistant
<small>e.g., Google Home, Amazon Alexa, Samsung SmartCam</small>	<small>e.g., Google, Amazon, Samsung</small>	<small>Alexa AI assistant</small>

Close Save Changes

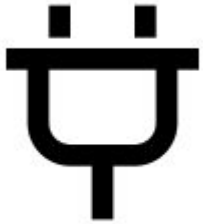
“ *What is this device doing?*”

Challenge 2: Communicating risks vs. spooking users

Difficult to infer remote hostnames due to missing DNS packets



Some hostnames could cause confusion

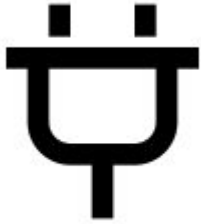


Belkin
Smart Plug



api.xbcs.net

Hostnames could also be spooky to some users



`tock.usno.navy.mil`

another
smart device

“

Why should I use and keep using IoT Inspector?

Challenge 3: Incentivizing users

User engagement can be improved



15,000+ devices labeled



2,900+ users labeled at least one device



63,000+ devices inspected



6,400+ users inspected at least one device

Median inspection time: 40+ minutes



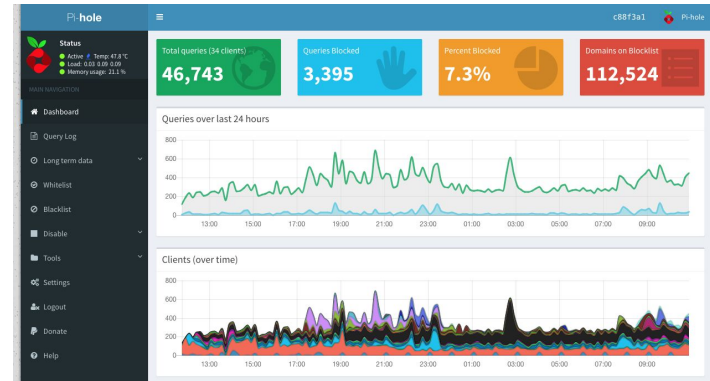
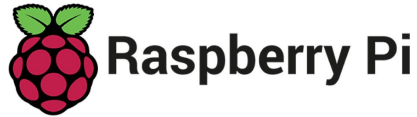
209,000+ devices scanned

Improving user experience

UI/UX

Provide more usable information

Platform



Analogue: Pi Hole

Need actionable use cases

Blocking

Blocking devices
Blocking connections

Hidden devices



Source: <https://twitter.com/foxytaughtyou/status/1536128978792198145/>

Challenges of 3 years of operating IoT Inspector

Identifying and labeling devices

Communicating risks

Letting users take actions

Incentivizing users

63,000+

devices

6,400+

users