Who Let the Smart Toaster Hack the House?
Exploring Security and Privacy Risks in Connected Devices

Anna Maria Mandalari
annamandalari.com
What if we are exchanging privacy for gimmicks and minor convenience?

What is IoT exposing when it comes to privacy in a **Smart Home**?

What might this mean for the future?
Why were we interested in this?

• They can (by definition) access the Internet and therefore may expose private information.

• They may listen to you (e.g., smart speakers).

• They may watch you (e.g., smart doorbells).

• They may know what you watch (e.g., smart TVs).

• They can (by definition) access the Internet and therefore may expose private information.

• Lack of understanding on what information they expose, on when they expose it, and to whom.

• Lack of understanding of regional differences (e.g., GDPR).

Smart TVs collect data about what you watch with a technology called ACR. Here’s how to turn it off.
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
What is IoT exposing when it comes to privacy in a Smart Home?
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
Goal of Research

What is the destination of IoT network traffic?

What information is sent?

Does a device expose information unexpectedly?
Google, Amazon, and Apple have decided to collaborate on a universal smart home ecosystem.

Amazon Echo

“I have their information”

Google

“And I have their privacy”

Apple

“So what are we waiting for”
210 devices in two different countries
Design of Experiments

- Controlled interactions
  - Automated (repeated 30 times)
    - Text-to-speech to smart assistants (Alexa/Google/Cortana/Bixby)
    - Monkey instrumented control from Android companion apps
  - Idle: background traffic

>200k Experiments

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>power on/off the device</td>
</tr>
<tr>
<td>Voice</td>
<td>voice commands for speakers</td>
</tr>
<tr>
<td>Video</td>
<td>record/watch video</td>
</tr>
<tr>
<td>On/Off</td>
<td>turn on/off bulbs/plugs</td>
</tr>
<tr>
<td>Motion</td>
<td>move in front of device</td>
</tr>
<tr>
<td>Others</td>
<td>change volume, browse menu</td>
</tr>
</tbody>
</table>
Data Collection Methodology

- Monitor all traffic at the **router**
  - per-device
  - per-experiment

Internet traffic is the only signal that (by definition) all IoT devices produce.
What Is the Destination?

1. DNS response
2. HTTP headers
3. TLS handshake

Network Traffic

Second-Level Domain (SLD)

Whois database (or common sense)

Organization

First party
Non-first party

IP Address

Destination IP

IP Owner

4. IP Owner

Geolocation

Same jurisdiction
Different jurisdiction

Passport
https://passport.oes.nau.edu
What Non-First Parties Are Contacted?

- Number of devices contacting non-first party organizations

<table>
<thead>
<tr>
<th>Organization</th>
<th>US</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>31</td>
<td>24</td>
</tr>
<tr>
<td>Google</td>
<td>14</td>
<td>9</td>
</tr>
<tr>
<td>Akamai</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>Microsoft</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Netflix</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Kingsoft</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>21Vianet</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Alibaba</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Beijing Huaxiay</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

- Nearly all TVs contact Netflix without being logged in.
- High reliance on cloud and CDN providers.
- Chinese cloud providers.

Regional differences.
Most devices contact outside testbeds’ privacy jurisdictions*
Other notable cases of activities detected when idle

Cameras reporting motion in absence of movement

Devices spontaneously restarting or reconnecting
WHEN ALEXA FINDS OUT YOU'VE BEEN LOOKING UP GOOGLE HOME
Are Smart Speakers Listening to Us?
What happens when the wake word is misunderstood?

I like the time...

Smart speakers signal **activation** (wake word detection) by **lighting up**

They **send the recording** to the voice assistant cloud service

The cloud service may **store the recording** and produce an answer

---

Google updates Home Mini to address major privacy bug

Some units of the smart speaker are found to activate at random times and transmit the audio to Google's servers.

---

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands.
Goals

Understanding when smart speakers *mistakenly record conversations*

- How frequent?
- Signaled?
- Do they adapt?
- For how long?
- Biases?
- Regionality?
- Which words?
Measurement challenges and solutions

How to expose smart speakers to content?
1. PLAY AUDIO FROM POPULAR SHOWS
   - 12 TV shows
   - 134 hours of video played two times in two regions

How to detect activations?
2. DETECT ACTIVATIONS
   - Camera recordings
     - Detects when a smart speaker lights up and for how long
   - Cloud data
     - Detects smart speaker recordings (only for Amazon and Google)
   - Network traffic
     - Detects traffic patterns resembling voice transmissions

How to distinguish unwanted activations?
3. RECOGNIZE MISACTIVATIONS
   - Analyze closed captions of each activation
     - Do they contain the wake word?
       - Yes
       - No
   - Legitimate activation
   - Misactivation!
Test environments

Coordinating server
- Plays audio content
- Provides WiFi
- Captures traffic
- Automates experiments

Testing cabinet
- Amazon Echo Dot 2nd gen. (Alexa)
- Amazon Echo Dot 3rd gen. (Alexa)
- Google Home Mini (Google Assistant)
- Apple Homepod (Siri)
- Harman Kardon Invoke (Cortana)
Activation detection methods

Camera activation
- search the video stream for frame changes

Traffic activation
- look for traffic spikes to certain destinations exceeding a certain threshold

Cloud activation: download information from the voice assistant cloud
- Only for Google Assistant and Amazon Alexa
How frequently do smart speakers misactivate?

Repeatability

- Consistency of misactivations across experiments

Takeaways

- Devices with the most recordings (Invoke, Echo2, Homepod) expose user privacy more often

- Prevalence of low repeatability suggests low determinism

Most misactivating devices

- invoke/cortana
- echo2/echo
- homepod/hey-siri
- echo2/amazon
- echo2/computer
- echo3/computer
- google/ok-google
- echo3/amazon
- echo3/echo
- echo2/alexa
- echo3/alexa

Number of distinct misactivations

Legend:
- 76-100% Repeatability
- 51-75% Repeatability
- 26-50% Repeatability
- 0%-25% Repeatability
How long do smart speakers record?

**Misactivation duration**: amount of time the smart speaker is lit up after a misactivation

- **Most common case (median)**
  - up to **4s** (Homepod, Echo Dot 2G)
- **Less common case (top 25%)**
  - up to **7s** (Homepod)
- **Rare case (top 10%)**
  - up to **10s** (Homepod)

*Enough to grasp a conversation?*
## What words cause most misactivations?

<table>
<thead>
<tr>
<th>Words</th>
<th>Some patterns</th>
<th>Some examples from the closed captions of highly repeatable misactivations</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK/Hey Google</td>
<td>Words rhyming with &quot;hey&quot;/&quot;hi&quot; followed by &quot;ol&quot;/&quot;g&quot;/&quot;w&quot;</td>
<td>&quot;Okay, where were we?&quot;, &quot;hey ... you told&quot;, &quot;A-P girl&quot;</td>
</tr>
<tr>
<td>Hey Siri</td>
<td>Words rhyming with &quot;hey&quot; or &quot;hi&quot; followed by voiceless &quot;s&quot;, &quot;f&quot;, &quot;th&quot; sound and &quot;i&quot;/&quot;ee&quot; vowel</td>
<td>&quot;yeah. I was thinking&quot;, &quot;Hi. Mrs. Kim&quot;, &quot;they ... secretly&quot;</td>
</tr>
<tr>
<td>Alexa</td>
<td>&quot;i&quot; followed by &quot;k&quot; sound or a voiceless &quot;s&quot;</td>
<td>&quot;I care about&quot;, &quot;I messed up&quot;, &quot;I got something&quot;</td>
</tr>
<tr>
<td>Echo</td>
<td>&quot;e&quot;/&quot;ee&quot;/&quot;i&quot; vowel followed by hard &quot;k&quot; or &quot;g&quot; sounds</td>
<td>&quot;head coach&quot;, &quot;I got&quot;, &quot;that cool&quot;, &quot;pickle&quot;</td>
</tr>
<tr>
<td>Computer</td>
<td>Words starting with &quot;comp&quot; or that rhyme with &quot;here&quot;</td>
<td>&quot;Comparisons&quot;, &quot;come here&quot;, &quot;nuclear accident&quot;</td>
</tr>
<tr>
<td>Amazon</td>
<td>Combinations of &quot;was&quot;/&quot;as&quot;/&quot;goes&quot;/&quot;some&quot;/&quot;I'm&quot; followed by &quot;s&quot;/&quot;z&quot;/&quot;on&quot;/&quot;om&quot;</td>
<td>&quot;it was a&quot;, &quot;life goes on&quot;, &quot;want some water?&quot;, &quot;I was in&quot;</td>
</tr>
<tr>
<td>Cortana</td>
<td>&quot;k&quot; sound closely followed by &quot;r&quot; or &quot;t&quot;</td>
<td>&quot;lecture on&quot;, &quot;quarter&quot;, &quot;courtesy&quot;, &quot;according to&quot;</td>
</tr>
</tbody>
</table>

- Most are wake word variations, no evidence of secret wake words
- Potential for some patterns to be used by an attacker to forge commands
WHEN YOU REALIZE
YOUR SMART HOME ISN'T SMART
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
Providers need to “identify” and “locate” IoT devices in the network.
Detecting IoT Devices at the Provider is Challenging

Traffic patterns across IoT devices are diverse

Deploying an agent inside at each ISP customers is not scalable

Active measurements do not work with devices behind NATs

Deep packet inspection raises privacy concerns

Our contribution: a methodology for **detecting** and monitoring IoT devices with **limited,** **passive,** and **sparsely sampled** flow data in the **wild.** (Detection rules available at [https://moniotrlab.ccis.neu.edu/imc20/](https://moniotrlab.ccis.neu.edu/imc20/))
Key Insights

- Devices have repeating patterns of communication that appear even in sparsely sampled data.

- Detection rules can be generated using limited packet fields.

- Detected devices from 77% of studied IoT manufacturers in an ISP and IXP within minutes to hours.
Methodology

1. Generate Ground Truth (GT) IoT Traffic
2. Check Visibility of GT at ISP Vantage Point
3. Identify Domains, IPs, and Port numbers and Generate Detection Rules
4. Cross check Detection Rules
5. Detect IoT Devices in the Wild
Generate Ground Truth IoT traffic

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>power on/off the device</td>
</tr>
<tr>
<td>Voice</td>
<td>voice commands for speakers</td>
</tr>
<tr>
<td>Video</td>
<td>record/watch video</td>
</tr>
<tr>
<td>On/Off</td>
<td>turn on/off bulbs/plugs</td>
</tr>
<tr>
<td>Motion</td>
<td>move in front of device</td>
</tr>
<tr>
<td>Others</td>
<td>change volume, browse menu</td>
</tr>
</tbody>
</table>

• Idle Experiments
• Active Experiments

56 different IoT products
ISP Setup

VPN GT from IoT labs to a Home (Home VP) in the ISP network and capture at ISP routers

15M broadband subscriber lines experiments
Generating Detection Rules

Detection Levels:

**Product-level:** Amazon Echo

**Manufacturer-level:** A Samsung Device

**Platform-level:** an IoT device

*Detection Rules:*

5 IoT Platforms
20 Manufacturers
11 Products
77% of the manufacturers in the testbeds
IoT devices talk to different domains at different rates
Some diurnal patterns for Alexa and Samsung IoT devices

1m+ subscribers with Alexa-enabled devices

Increasing observation period helped detecting more devices

IoT activity for ~20% of ISP subscriber lines
Detecting IoT Devices Activity in the Wild

For some devices we can infer activity
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
I DON'T ALWAYS THINK ABOUT CYBER SECURITY

BUT WHEN I DO, IT'S TOO LATE
Contributions

• We develop an automated methodology for evaluating security vulnerabilities in common consumer IoT devices using large-scale, diverse experiments and sets of attacks

• We assess the security vulnerabilities of popular IoT devices against existing network and device attacks and identify privacy risks
Assumptions

• Threat modelling
  • *Adversary*: Any party that can access the IoT device’s network
  • *Victim*: The victim is anyone who enters the service area of the IoT device
  • *Threat*: We assume the presence of malicious or compromised IoT devices in a smart home. Adversaries may be incentivised to compromise other devices in the network to infer user activities or deny their usage of them.

• Goals
  • *Are consumer IoT devices vulnerable to common security attacks?*
  • *Do IoT devices detect threats?*

• Non-goals
  • We have no control over how an IoT device works internally.
  • We do not test all threats.
  • We only focus on consumer IoT devices.

Testbed
## Testbed

<table>
<thead>
<tr>
<th>Category</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart speaker</td>
<td>Bose Smart Speaker 500</td>
</tr>
<tr>
<td></td>
<td>Sonos One (Gen2)</td>
</tr>
<tr>
<td></td>
<td>Echo Dot 5</td>
</tr>
<tr>
<td>Smart doorbell</td>
<td>Ring Chime Pro</td>
</tr>
<tr>
<td></td>
<td>Ring Video Doorbell (2nd Gen)</td>
</tr>
<tr>
<td>Smart camera</td>
<td>Google Nest Cam</td>
</tr>
<tr>
<td></td>
<td>SimpliSafe Security Camera Indoor</td>
</tr>
<tr>
<td></td>
<td>Furbo 360° Dog Camera</td>
</tr>
<tr>
<td>Appliances</td>
<td>WeeKett Smart Wi-Fi Kettle</td>
</tr>
<tr>
<td></td>
<td>Govee Alexa LED Strip Lights</td>
</tr>
<tr>
<td></td>
<td>Sensibo Sky Smart AC</td>
</tr>
</tbody>
</table>
### Testbed

- **Within the same LAN**
- **Packets are captured on the access point**
- **Tshark for filtering responses**
- **Assess device reaction**
  - Counter-measures detected – attack **unsuccessful**
  - No counter-measures detected – attack **successful**

### Attacks

<table>
<thead>
<tr>
<th>Category</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flooding</td>
<td>SYN (port 80) flooding</td>
</tr>
<tr>
<td></td>
<td>UDP flooding</td>
</tr>
<tr>
<td></td>
<td>DNS flooding</td>
</tr>
<tr>
<td></td>
<td>Fragmented IP flooding</td>
</tr>
<tr>
<td>Scanning</td>
<td>Port scanning</td>
</tr>
<tr>
<td></td>
<td>OS scanning</td>
</tr>
</tbody>
</table>

- Mock Attacker
- Access Point
- Internet
- Mock Attacker
- Target IoT Devices

- LAN
- WAN
Software

• We write and use configurable and automated scripts for simulating attacks and analysing the replies
• We setup tcpdump to continuously capture network traffic on the network access point
• Dedicated network traffic capturing for active experiments
• Devices are activated with their companion applications remotely and automatically using ADB
• We verify the attacks using two RPIs
Software – testing usecase

• Activate the device with ADB
• Start running a simulated attack on the device’s IP address
• Wait until the attack stops
• Download the captured traffic
• Analyse the traffic using tshark
## Results - flooding

<table>
<thead>
<tr>
<th>Devices</th>
<th>SYN</th>
<th>UDP</th>
<th>DNS</th>
<th>Frag. IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bose Speaker</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Sonos One (Gen2)</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Echo Dot 5</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Ring Chime Pro</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Ring Doorbell</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Google Nest Cam</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>SimpliSafe Cam</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Furbo Camera</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>WeeKett Kettle</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Govee Lights</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Sensibo Sky</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- Most of the devices are vulnerable to Frag. IP flooding, as opposed to SYN flooding, which is only successful on the Bose Speaker.
Results – port scanning

- Open ports can be detected on 7 devices out of 11.

<table>
<thead>
<tr>
<th>Devices</th>
<th>Identified Open Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bose Speaker</td>
<td>80/7000/8082/8083/8085/8091/8200/30030/40002/40031/40035</td>
</tr>
<tr>
<td>Sonos One (Gen2)</td>
<td>1400/1410/1443/1843/7000</td>
</tr>
<tr>
<td>Echo Dot 5</td>
<td>1080/4070/8888/55442/55443</td>
</tr>
<tr>
<td>Ring Doorbell</td>
<td>Blocking ping probes &amp; none found</td>
</tr>
<tr>
<td>Google Nest Cam</td>
<td>8012/10101/11095</td>
</tr>
<tr>
<td>SimpliSafe Cam</td>
<td>19531</td>
</tr>
<tr>
<td>Furbo Camera</td>
<td>None found</td>
</tr>
<tr>
<td>WeeKett Kettle</td>
<td>6668</td>
</tr>
<tr>
<td>Govee Lights</td>
<td>None found</td>
</tr>
<tr>
<td>Sensibo Sky</td>
<td>None found</td>
</tr>
</tbody>
</table>
### Results – OS scanning

<table>
<thead>
<tr>
<th>Devices</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bose Speaker</td>
<td>Linux 3.2 - 4.9</td>
</tr>
<tr>
<td>Sonos One (Gen2)</td>
<td>Linux 3.2 - 4.9</td>
</tr>
<tr>
<td>Echo Dot 5</td>
<td>No exact match, can be Linux</td>
</tr>
<tr>
<td>Ring Chime Pro</td>
<td>Too many fingerprints match</td>
</tr>
<tr>
<td>Ring Doorbell</td>
<td>2N Helios IP VoIP doorbell (95%)</td>
</tr>
<tr>
<td>Google Nest Cam</td>
<td>Too many fingerprints match</td>
</tr>
<tr>
<td>SimpliSafe Cam</td>
<td>Too many fingerprints match</td>
</tr>
<tr>
<td>Furbo Camera</td>
<td>Too many fingerprints match</td>
</tr>
<tr>
<td>WeeKett Kettle</td>
<td>No exact OS matches</td>
</tr>
<tr>
<td>Govee Lights</td>
<td>Espressif esp8266 firmware (lwIP stack), NodeMCU firmware (lwIP stack)</td>
</tr>
<tr>
<td>Sensibo Sky</td>
<td>Philips Hue Bridge (lwIP 1.4.1), Philips Hue Bridge (lwIP stack)</td>
</tr>
</tbody>
</table>

- OS can be identified on 5 devices out of 11.
Discussion

• Potentially consequential user implications can be identified (e.g. a successful DoS attack on the LED light)
• Open ports and identified OS could be exploited for obtaining private info (e.g. camera feed)
• Limitations
  • We consider devices as black-boxes
  • We only tested 11 devices
• Ethical considerations
  • We follow the ethical guidelines of our affiliated organisation
  • We conduct our experiments locally
Install IoT security camera

camera has security flaw

strangers can watch the video feed

strangers can watch the video feed
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
Problem: IoT Devices Expose Information Over the Internet

They “sense” a lot
- Microphones
- Cameras
- User activities
  ...

Privacy Threats
- IoT devices collect user information
- They share user information

Security Threats
- Malware can affect IoT devices
- An attacker can control them

User Frustration
- IoT devices privacy/security is hard to control
- Hard to protect users from IoT threats
IOT PROTECTION SYSTEMS: SAFEGUARDS
Why Were We Interested in This?

- These safeguards may currently be ineffective in preventing risks.
- Their cloud interactions and data collection operations may introduce privacy risks.
Research Questions

- **Goal 1:** What are the privacy and security implications on how a safeguard works?

- **Goal 2:** Do the safeguards detect threats?

- **Goal 3:** What are the side effects of the safeguards?

**IoT Safeguards**
Challenges for Measuring IoT Safeguards

Difficult to automate the testing of commercial IoT safeguards

• Closed systems
• Blackbox approach

Difficult to perform IoT experiments and generalize

• Lack of automation and emulation tools
• Lack of standard testbed

Our contribution: a large IoT testbed used to test IoT safeguards in real-world scenarios (software and data available online).
Selecting IoT Safeguards

ISP / Internet / Cloud Services

Safeguard

IoT-LAN

Software Safeguard

ISP/Internet/Cloud

Home Router

IoT-LAN

Router Safeguard

ISP/Internet/Cloud

Home Router

IoT-LAN

Bridge Safeguard

ISP/Internet/Cloud

Home Router

IoT-LAN

ARP-Spoofing Safeguard

ISP/Internet/Cloud

Home Router

IoT-LAN

Add-on Software

Safeguard

NAT

McAfee

Bitdefender

Firewalla

RATtrap

Avira SafeThings™

F-Secure

Fing
Testbed

- **ISP / Internet**
- **Gateway**
- **LAN**
- **Safeguard**
  - Android Phone
  - Safeguard notifications and threat detection
- **IoT-LAN**
- **IoT Bridge**
- **L2 Bridge**
- **IoT Devices**
  - Packet capture and threat simulation
Goal 1: What are the privacy and security implications on how a safeguard works?

- **Identify locality**: cloud vs local operation
- **Operation**: usage third-party services to operate
Processing Locality & Party Characterization

Safeguards Network Traffic

Second-Level Domain (SLD)

Organization

First party

Non-first party

Whois database (or common sense)

IoT Traffic

Traffic to the safeguards destinations

Local

Cloud
### Processing Locality & Party Analysis

<table>
<thead>
<tr>
<th>Safeguard</th>
<th>Destinations #</th>
<th>Cloud</th>
<th># and list of Support/3rd Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avira</td>
<td>10</td>
<td>Yes</td>
<td>(1) api.mixpanel.com</td>
</tr>
<tr>
<td>Bitdefender</td>
<td>5</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>F-secure</td>
<td>1</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>FingBox</td>
<td>5</td>
<td>Yes</td>
<td>(2) api.snapcraft.io, mlab-ns.appspot.com</td>
</tr>
<tr>
<td>Firewalla</td>
<td>4</td>
<td>No</td>
<td>(1) api.github.com</td>
</tr>
<tr>
<td>McAfee</td>
<td>22</td>
<td>Yes</td>
<td>(3) app-measurement.com, commscope.com, avast.com</td>
</tr>
<tr>
<td>RatTrap</td>
<td>1</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>TrendMicro</td>
<td>3</td>
<td>Yes</td>
<td>(1) policy.ccs.mcafee.com</td>
</tr>
</tbody>
</table>

**Take away:**
- Usage of the cloud for performing analysis, potentially leaving the user vulnerable in the event of a data breach.
- Destinations contacted that are not first parties.
IoT Device Identification

Protection techniques applied to specific vendors

percentage of IoT devices is correctly identified.
Research Questions

- **Goal 2:** Do the safeguards detect threats?
  - Safeguards **notify** the user when detecting privacy or security threats.
Testing Threat Detection Capability

- **Security**
  - Anomalous behavior
  - Open Port
  - Weak Password
  - Device Quarantine
  - DoS attacks
  - Port/OS Scanning
  - Malicious Destinations

- **Privacy**
  - PII Exposure
  - Unencrypted Traffic
  - DNS over HTTPS
Threat Detection Experiments

- start (d=0)

  - Simulate a threat: run threat simulation script

  - Wait 20 minutes to allow threat detection

  - Check if the safeguard detects the threat: run threat detection script
    - threat detected \( (d=d+1) \)
    - threat not detected

  - Is this the 30th iteration?
    - Yes \( (d \geq 1) \)
      - The safeguard can detect the threat
    - No
      - Yes \( (d < 1) \)
        - The safeguard cannot detect the threat

<table>
<thead>
<tr>
<th>Threat</th>
<th>Avira</th>
<th>Bitdefender</th>
<th>F-Secure</th>
<th>Fingbox</th>
<th>Firewalla</th>
<th>McAfee</th>
<th>RaTtrap</th>
<th>TrendMicro</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anomaly ON/OFF</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Anomaly Traffic Pattern</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Abnormal Upload</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Open Port</td>
<td>X</td>
<td>✓ (30s)</td>
<td>-</td>
<td>-</td>
<td>✓ (30s)</td>
<td>X</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Weak Password</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Device Quarantine</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>SYN Flooding</td>
<td>X</td>
<td>✓ (30s)</td>
<td>X</td>
<td>-</td>
<td>✓ (40s)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>UDP Flooding</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DNS Flooding</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HTTP Flooding</td>
<td>X</td>
<td>✓ (3m)</td>
<td>-</td>
<td>-</td>
<td>✓ (2m)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IP Fragmented Flood</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Port Scanning</td>
<td>✓ (45s)</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>✓ (30s)</td>
</tr>
<tr>
<td>OS Scanning</td>
<td>✓ (45s)</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Malicious Destinations</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>-</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>PII Exposure</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Unencrypted Traffic</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DNS over HTTPS</td>
<td>X</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Take away:** - only 3 out of 14 threats are detected by the safeguards. 3 out of 8 safeguards do not detect any threats at all, despite they claiming to do so in their specifications. - Some of safeguards take between 45 seconds and 3 minutes to detect a security threat.
Goal 3: What are the side effects of the safeguards?

- Traffic overhead, overprotection, privacy implications
Safeguard Side Effects

Overprotection

CONNECT 12 IOT DEVICES TO THE SAFEGUARDS AND CAPTURE THE TRAFFIC FOR ONE MONTH

Network traffic overhead

Privacy Policy

MANUALLY INSPECTING THE PRIVACY POLICY
Overprotection

Take away: Most safeguards do not overprotect (i.e., they do not report threats that do not occur).
Traffic Overhead

Take away: Some of the safeguards introduce significant traffic overhead. In general the overhead is never less than 10% of the traffic of the IoT devices.
## Privacy Policy

<table>
<thead>
<tr>
<th>Privacy Policy</th>
<th>Avira</th>
<th>Bitdefender</th>
<th>F-Secure</th>
<th>Fingbox</th>
<th>Firewalla</th>
<th>McAfee</th>
<th>RaTtrap</th>
<th>TrendMicro</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymization</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓ [pseudonymize]</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Usage of Personal Data</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Retention Period</strong></td>
<td>In accordance with legal requirements</td>
<td>10 years</td>
<td>6 months</td>
<td>As long as necessary</td>
<td>Indefinitely</td>
<td>Subscription period</td>
<td>Subscription period</td>
<td>Ongoing legitimate business need</td>
</tr>
<tr>
<td><strong>Third Party</strong></td>
<td>SaaS vendor, Akamai, Mixpanel, Ivanti</td>
<td>Partners</td>
<td>Partners</td>
<td>Partners</td>
<td>✗</td>
<td>Partners</td>
<td>Partners</td>
<td>Partners</td>
</tr>
</tbody>
</table>

**Take away:** Most user information is shared with third-party entities, sometimes without anonymization. Sharing data outside user’s privacy jurisdiction.
57% (50%) of destinations of the US (UK) devices are not first-party
Why is this a problem?

Profiling

Mass-influence

User emotion
TODAY SECURITY ENGINEER SITUATION

DEAR HACKERS PLS DON'T DO ANYTHING TODAY!
What might this mean for the future?
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
THE INTERNET OF THINGS

WHAT COULD POSSIBLY GO WRONG?
Solution at the Edge

Goal 1: methodology
- IoT device
- Test device functionality while blocking a destination
- Required Destinations: blocking them breaks functionality
- Non-required Destinations: blocking them does not break functionality

Goal 2: measurement
- Non-essential traffic
- IoTTrimmer
- Essential traffic

Goal 3: mitigation

/ Generalizable
/ Self adaptive
/ Accurate IoT blocker
Idea

• What we learn: some IoT traffic is **essential** and some of it is **non-essential**

• Can we (partially) "silence" IoT devices and still be able to enjoy them?
Goals

• *Measurement Methodology*: How to automatically separate essential traffic from non-essential traffic?

• *Identification*: How prevalent is non-essential traffic in our testbed of 31 IoT devices?

• *Generalizations*: Are there any common patterns in non-essential traffic?

• *Mitigation*: How to build a system for filtering non-essential traffic?
Challenges

• IoT devices are **hard to test** automatically
  • They offer very different functionalities
  • They suffer (in our experience) from frequent service outages that must be detected
  • They typically require user interaction (i.e., they are not directly programmable)
  • Hard to verify if a functionality was actually executed or not

• Ideas:
  • use **companion devices** (phones and voice assistants)
  • use **network traffic patterns** to classify IoT devices responses
Measurement Methodology

Hardware and Software of our IoT testbed

- IoT devices
  - 31 in total: 6 cameras, 15 home automation, 5 smart hubs, 3 smart speakers, 2 video
- Router with IP filtering and DNS filtering capabilities
- Power plugs and scripts to power cycle the devices
- Trigger scripts to invoke IoT devices functionality
  - Companion app interaction and voice assistant interaction
- Probe scripts to detect success or failure in functionality execution
  - Compare companion app screenshots and identification of traffic peaks
Functionality Experiment

- Goal: determine if a functionality works

- Test the functionality at least 10 times

- Terminate if 80% consensus is reached

- When tested 30 times against ground truth, probes have been 80% correct

- If probes are 80% correct, the chance of an incorrect functionality experiment result is less than 0.01%
Identifying Non-essential Traffic
Distinguishing Required from Non-Required Destinations

• Goal: determine if a destination is required (i.e., if its traffic is essential)

• Block destinations one by one

• If the functionality succeeds when a destination is blocked, such destination is non-required

• Otherwise it is required
Overall Results

Devices with at least one non-required destination

- 16/31 devices have non-essential traffic
- Mostly cameras, smart speakers, and video
- Possible explanations:
  - complexity (skills and apps)
  - uncommon vendors / rebranding (for cameras)
## Required vs. Non-required Destinations

<table>
<thead>
<tr>
<th>Device</th>
<th># of Destinations</th>
<th>Required</th>
<th>Non-Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blink-camera</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Bosiwo-camera</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Icsee-doorbell</td>
<td>6</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Reolink-cam</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Wansview-cam</td>
<td>9</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Yi-camera</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td><strong>Home-automation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App-kettle</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Honeywell-thermostat</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Magichome-strip</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Meross-dooropener</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Nest-tstat</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Netatmo-weather-station</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Smarter-coffee-mach</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Smartlife-bulb</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Smartlife-remote</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Sousvide</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Switchbot</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Tplink-bulb</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Tplink-plug</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Wemo Plug</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Xiaomi-ricecooker</td>
<td>7</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th># of Destinations</th>
<th>Required</th>
<th>Non-Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart-hub</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insteon-hub</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Lightify-hub</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Philips-hub</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Samsung Hub</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Sengled-hub</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td><strong>Smart-Speaker</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allure-speaker</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Echodot</td>
<td>10</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Google-home</td>
<td>9</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FireTV</td>
<td>14</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>Roku TV</td>
<td>10</td>
<td>2</td>
<td>8</td>
</tr>
</tbody>
</table>
**Total**              | **119**           | **57**   | **62**       |

- Non-required destinations are contacted the most by cameras, speakers, and video devices.
- But it also happens on simpler devices such as the TP-Link smart plug and smart bulb.
Amount of Data Sent During One Experiment

- **Good news**: non-essential traffic is relatively small (less than 1KB/device)
- However, it is still possible to transmit:
  - Presence of the device
  - Its status
  - Basic data from the sensors (e.g., open/close, motion/still, alarm/no alarm)
Similarities with Existing Blocklists

- We consider Pi-hole, Firebog, MoAB, StopAD lists
- No required destinations on such lists
- Up to 6 out of 62 non-required destinations present in existing blocklists
- Public blocklists are of limited help in blocking IoT non-essential traffic

<table>
<thead>
<tr>
<th>Device</th>
<th>Non-req Dest.</th>
<th>Pi-hole</th>
<th>Firebog</th>
<th>MoAB</th>
<th>StopAd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allure Speaker</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bosiwo Camera</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Echo Dot</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fire TV</td>
<td>11</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Google Home</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Isee Doorbell</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nest Thermostat</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Philips Hub</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reolink Camera</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Roku TV</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Samsung Hub</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TP-Link Bulb</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TP-Link Plug</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wansview Camera</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Xiaomi Ricecooker</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>YI Camera</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Mitigating Non-essential IoT Traffic

• A blocking system: **IoTrim**
  • Filtering router between the IoT devices and the Internet
  • Block/allow lists based on (non-)required destinations → crowdsourced
  • Software to declare device types and manage the lists / blocking rules
  • A proof-of-concept prototype is available for download
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
Motivation

- Inefficiency of existing IoT solutions
- Most of them are cloud-based: might share users’ personal/sensitive data

Research Questions

- Can we replace cloud-based IoT protection systems by a local IDS/IPS running on a home router?
- If so, what is the performance overhead?

Benefits

- **Security improvement**: cover wider spectrum of IoT threats in a home network
- **Privacy improvement**: All users’ data processed locally and not shared with cloud
SunBlock Architecture

Al-based Network Threat Detection Module

- Feature Extraction
- Model Training & Update
- Threat Detection

Traffic Inspector
- Rules

Traffic Filtering

Rule-based Traffic Filtering Module

Raw Traffic

Filtered Traffic

Home Router
Implementation: home router with IoT protection

- LinkSys WRT3200ACM, OpenWRT Linux-based OS
- ~4GB flash, 512MB swap (for ML training only), 512 MB RAM
- Snort3 for rule-based filtering, netml with OCSVM for AI-based module

Testbed

- 10 most popular IoT device types (according to IoT Inspector paper)
- Smart speakers (Echo spot, Google Home), Video (FireTV), Camera (Yi, Blink), Home automation (Nest thermostat, TP-Link/Wemo plugs, Gosund/TP-Link bulbs)
- Devices were triggered daily using the methodology similar to the S&P paper
Evaluation: threat coverage and prevention time

<table>
<thead>
<tr>
<th>Threat</th>
<th>IoT Protection Systems</th>
<th>SunBlock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomalous Traffic</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Anomalous Upload</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SYN Flooding</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UDP Flooding</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>DNS Flooding</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>HTTP Flooding</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Port Scanning</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OS Scanning</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PII Leakage</td>
<td>X</td>
<td>✓</td>
</tr>
</tbody>
</table>
Evaluation: performance overhead

Model training

<table>
<thead>
<tr>
<th>Protection Level</th>
<th>CPU (%)</th>
<th>RAM (MB)</th>
<th>swap (MB)</th>
<th>Training Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule-based &amp; AI-based</td>
<td>18 ± 3</td>
<td>444 ± 4</td>
<td>296 ± 21</td>
<td>924 ± 253</td>
</tr>
<tr>
<td>AI-based only</td>
<td>26 ± 2</td>
<td>442 ± 6</td>
<td>197 ± 28</td>
<td>429 ± 171</td>
</tr>
<tr>
<td>Rule-based only</td>
<td>32 ± 4</td>
<td>423 ± 9</td>
<td>132 ± 20</td>
<td>180 ± 22</td>
</tr>
<tr>
<td>Unprotected</td>
<td>39 ± 2</td>
<td>410 ± 3</td>
<td>55 ± 1</td>
<td>113 ± 10</td>
</tr>
</tbody>
</table>

Regular IoT traffic

HTTP flood

UDP flood
Takeaways

• IoT threats can be rapidly detected on a home router with Rule&AI-based filtering algorithms

• No need in cloud-based solutions and in sharing your personal data

• Increase in CPU and RAM doesn’t affect main router functions leaving plenty of free resources: >50% free CPU and ~30% free RAM

• Further plans: beta testing and precise performance benchmarking against existing IoT solutions
OUR DEVICES ARE NOW 100% SECURE.

I TURNED THEM ALL OFF.

HOW DID YOU DO THAT?
Strengthening the IoT Ecosystem

**Trust**
- Endpoints’ practices
- Trusted platform modules
- Domain-specific guidelines and frameworks
- Access networking system & machine learning

**Interconnectivity**
- Understand threats in real world scenario
- Inferences on crowdsourced IoT data
- New secure IoT (wireless) networking protocols & systems
- Privacy preserving technologies at the edge

**Awareness, Authentication & Management**
- Usable monitors for IoT
- Context-aware privacy
- Personalised privacy
Is Your Kettle Smarter Than a Hacker?

• Assessing Replay Attack Vulnerabilities on Consumer IoT Devices using AI
  • Automated methodology for large-scale testing replay attack vulnerabilities on IoT devices
  • Using AI for detecting the success of the attack
Methodology

**STEP 1**  
(Sniff messages)

**STEP 2**  
(Flows organization)

**STEP 3**  
(Stack construction)

**STEP 4**  
(Replay attack)

**STEP 5**  
(Queue construction)

**STEP 6**  
(Attack detection)

- Companion App
- IoT Device

---

**Flow 1**: 
- $A_1 \rightarrow A_2$
- $B_1 \rightarrow B_2$
- $C_1 \rightarrow C_2$
- $C_3$

**Flow 2**: 
- $B_1 \rightarrow B_2$
- $B_3$

**Flow 3**: 
- $C_1 \rightarrow C_2$
- $C_3$

<table>
<thead>
<tr>
<th>STACK</th>
<th>REPLIoT</th>
<th>IoT Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow 3</td>
<td>$C_1 \rightarrow C_2$</td>
<td>$C_3$</td>
</tr>
<tr>
<td>Flow 2</td>
<td>$B_1 \rightarrow B_2$</td>
<td>$B_3$</td>
</tr>
<tr>
<td>Flow 1</td>
<td>$A_1 \rightarrow A_2$</td>
<td>$A_3$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUEUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\overline{B}_2$</td>
</tr>
<tr>
<td>$j = 2$</td>
</tr>
<tr>
<td>$\overline{B}_3$</td>
</tr>
<tr>
<td>$\overline{A}_2$</td>
</tr>
</tbody>
</table>

- Response Check
  - yes → SUCCESSFUL
  - no → FAILED

- Protocol Check
  - yes → FAILED
  - no → FAILED

- Any regular responses?
  - yes → FAILED
  - no → SUCCESSFUL
Methodology

use the **CheckLocalConnectivity** script to verify if the device leverages the local network

- **any local traffic captured?**
  - no
  - sniff the traffic while the device is set in the **OBVERSE / REVERSE** state via the **TrainingModule**
  - train ML models via the **TrainingModule**
  - sniff the traffic while the device is set in the **OBVERSE** state via the **AttackModule** then set it in the **REVERSE** state
  - **Restart Scenario?**
    - no
    - perform the replay attack via the **AttackModule** and then invoke the **DetectionModule** with \( j=3 \)
  - yes
  - restart the device via the **RestartDevice** script

- yes
**Replay Attack Results. ✓ indicates whether the replay attack is successful or not (X).**

<table>
<thead>
<tr>
<th>Device (<em>Tested via APIs</em>)</th>
<th>Non-Restart Scenario</th>
<th>Restart Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yeeligth lightstrip</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Yeelight bulb</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wiz lighthbulb</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lix bulb</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lepro bulb</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Govee lightstrip *</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Nanoleaf triangle *</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tapo smartplug</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Meross smartplug</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WeeKett Kettle</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Eufy robovac 30C</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OKP vacuum</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iRobot roomba i7</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sonos Speaker *</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bose Speaker *</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wyze cam pan</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Vtech baby monitor</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Boyfun Baby monitor</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Furbo camera</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Meross Garage Opener</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Many thanks for your valued reply.

After confirming with our security team, the vulnerability has been resolved in the latest firmware of P110.

Since this firmware is currently in gray release, we are not sure whether your P110 could receive the firmware right now, you could check it in Tapo App.

If there is no firmware update for your P110, please provide the MAC address with us, we will release the firmware for your P110 and hope you could help verify the remediation work in the latest firmware.

If you have additional concerns or information, please feel free to let us know. If you have any subsequent plan or processing of the vulnerability, we also hope that you can further synchronize to us.

Thank you for your cooperation and patience.

Ian.xu
TP-Link Technical Support

----------------------------------------
Website: https://www.tp-link.com/support/
Feedback: Report a suggestion/complaint on this email service by clicking here
Why Were We Interested in This?

- These devices may introduce privacy and security risks.
- Their cloud interactions and data collection operations may introduce privacy risks.
Goal 1: Develop a system able to inject realistic anomalies for healthcare IoT devices.

Goal 2: Explore how the time window used for training affects the accuracy of the anomaly detection, for three different types of anomalies.

Goal 3: Demonstrated that training the model at the edge of the network on a representative edge device (Raspberry Pi) is feasible.
Challenges for Measuring IoT Devices

Difficult to automate the testing of commercial IoT safeguards

• Closed systems
• Blackbox approach

Difficult to perform IoT experiments and generalize

Our contribution: a system for injecting and detecting IoT anomalous behavior in real-world scenarios (software and anomaly data available online).

• Lack of standard testbed
Dataset

- Collected by the UK Dementia Research Institute and Technology Centre (UK DRI).

- In-home activity of people living with dementia (PLWD), from motion sensors, wearable devices and physiological measurements.

- 44 different households, each fitted with 22 IoT devices.
## Dataset

<table>
<thead>
<tr>
<th>Function</th>
<th>Format</th>
<th>IoT Device</th>
<th>Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Binary</td>
<td>WC, bathroom, bedroom, corridor, dining room, hallway, kitchen, living room, lounge, office, study</td>
<td>-</td>
</tr>
<tr>
<td>Door</td>
<td>Binary</td>
<td>back door, conservatory, fridge door, front door, garage, main door, secondary, utility</td>
<td>✓</td>
</tr>
<tr>
<td>Appliances</td>
<td>Binary</td>
<td>iron use, kettle use, microwave use, socket use, toaster use</td>
<td>-</td>
</tr>
<tr>
<td>Temperature</td>
<td>Float</td>
<td>temperature, body temperature, skin temperature</td>
<td>✓</td>
</tr>
<tr>
<td>Health Related</td>
<td>Float</td>
<td>blood pressure, body mass index, body muscle mass, body weight, heart rate, body fat, body water, bone mass</td>
<td>-</td>
</tr>
<tr>
<td>Light</td>
<td>Integer</td>
<td>light level</td>
<td>✓</td>
</tr>
<tr>
<td>Sleep Event</td>
<td>Binary</td>
<td>sleep event, sleep mat snoring</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Float</td>
<td>sleep mat heart rate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integer</td>
<td>sleep mat respiratory rate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>sleep mat state, agitation</td>
<td></td>
</tr>
</tbody>
</table>
Threat Model

**Victim:** A person that uses a healthcare IoT device.

**Adversary:** Any party with access to the IoT device Traffic.

**Threat:**
- Adversaries may be incentivized to share privacy-sensitive information of patients.
- Malicious attacks hijack the communication channel, modifying the data sent by the IoT device.
Types of anomalies

On-off:
- For Binary sensors (i.e switches, doors)
- Recreates a sensor which repeatedly switches on and off.

Variance:
- For sensors which record floats or integers (i.e thermometer, blood pressure)
- Recreates noise or randomized readings.

Spike:
- For sensors which record floats or integers
- Recreates a random abnormal spike in the readings

<table>
<thead>
<tr>
<th>Anomaly</th>
<th>IoT device</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Off</td>
<td>Room Location, Appliance Use, Sleep Event</td>
</tr>
<tr>
<td>Variance</td>
<td>Ambient Temp, Body Temp, Light</td>
</tr>
<tr>
<td>Spike</td>
<td>Sleep Respiratory, Hearth Rate, Sleep Hearth Rate</td>
</tr>
</tbody>
</table>

“Variance anomaly injected in the Light intensity sensor for 4 days”
System Design

- Edge Inference Engine 1
- Edge Inference Engine 2
- Edge Inference Engine ...
- Edge Inference Engine n

- IoT Data
- Client 1
- Client 2
- Client ...
- Client n

- Local Analysis
- Anomaly Detection

- Anomaly Injection
Overview of Methodology

- **Data Loader**
  - Options:
    - Select specific patients.
    - Select one or multiple patients.

- **Anomaly Injection**
  - Options:
    - Type of anomaly.
    - Number of anomalies.
    - Time window length that anomalies will be injected in.

- **Data Pre-Processing**
  - Options:
    - Sliding time window.
    - Train, Valid. split based on time window.
    - Features: Sensor readings, Time interval between readings ($\delta t$).

- **Model Inference**
  - Architectures tested: DNN, CNN, KNN.
  - Library used: PyTorch.
  - Early stopping for training.
  - Unsupervised Learning.

- **Anomaly Detection**
  - The average training loss of the final epoch is calculated.
  - Multiplied by a coefficient, it acts as the threshold to detect anomalies.
Anomaly Detection Accuracy

Take away: On-Off Anomaly. The anomaly detection accuracy changes with training window size and different validation window sizes.
Take away: A model updated using data from one patient does not perform well on another patient and vice versa.

Average accuracy across all patients while training and validating with the same and different patients.
Personalized Models

Take away: The accuracy decreases when training the model with all patients. This shows that a model updated with data specific to each patient will achieve better performance.

Average accuracy across all patients while training with all patients and validating with one patient, compared to training with all and validating with one patient.
Course Overview

- Benchmarking privacy in IoT devices
- IoT devices identification
- Benchmarking security in IoT devices
- Benchmarking security solutions for IoT devices
- Privacy solutions for IoT devices at the edge
- Security solutions for IoT devices at the edge
- IoT devices certification scheme

The Problem

- 21.5 billion IoT devices in the world
- They have access to user private information
- They are a threat for user privacy and security
Mitigation

- Regularly train the ML models at the edge to keep up with the changes in device usage trends

- Approaches that rely on local traffic analysis: edge-based solutions running on the home gateway
WHEN YOU SEE HOW SOPHISTICATED CYBERTHREATS HAVE BECOME
COPSEC: Compliance-Oriented IoT Security and Privacy Evaluation Framework

Cybersecurity guidelines* such as ENISA, NIST, IoT Regulation Policy (UAE) have been released for improving IoT design practice.

Privacy regulations** such as GDPR (in EU) and CCPA (in California)

There is a lack of understanding whether IoT devices comply with them.

*NOT mandatory
**Mandatory
Motivation

• In 2023 the Cyber Resilience Act (in EU) and the US Cyber Trust Mark (in US) make further step towards a certification program of smart devices

• For consumer IoT devices, the certification process is thought as a self-assessment performed by the vendors themselves

• Should we trust vendors?
Methodology

1. Select security guidelines and privacy regulations
2. Turn them into metrics
3. Define experiments to test the extracted metrics on IoT devices
4. Produce a certification label for the tested device
## Results

<table>
<thead>
<tr>
<th>Device</th>
<th># of Unused Open Ports</th>
<th># of Unrecognized Protocols</th>
<th>Compliant with GDPR Art. 32 (a)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bose Speaker</td>
<td>(11 ports)</td>
<td>(0 protocols)</td>
<td>✔️</td>
</tr>
<tr>
<td>Echo Dot 5</td>
<td>(5 ports)</td>
<td>(3 protocols)</td>
<td>✔️</td>
</tr>
<tr>
<td>Furbo Dog Camera</td>
<td>(0 ports)</td>
<td>(1 protocol)</td>
<td>✔️</td>
</tr>
<tr>
<td>Google Nest Cam</td>
<td>(3 ports)</td>
<td>(1 protocol)</td>
<td>✔️</td>
</tr>
<tr>
<td>Govee lights</td>
<td>(0 ports)</td>
<td>(0 protocols)</td>
<td>✔️</td>
</tr>
<tr>
<td>Ring Video Doorbell</td>
<td>(0 ports)</td>
<td>(2 protocols)</td>
<td>✔️</td>
</tr>
<tr>
<td>Sensibo Sky Sensor</td>
<td>(0 ports)</td>
<td>(0 protocols)</td>
<td>✔️</td>
</tr>
<tr>
<td>SimpliSafe Cam</td>
<td>(1 ports)</td>
<td>(0 protocols)</td>
<td>✔️</td>
</tr>
<tr>
<td>Sonos One</td>
<td>(5 ports)</td>
<td>(1 protocol)</td>
<td>(mac in the clear)</td>
</tr>
<tr>
<td>WeeKett Kettle</td>
<td>(1 ports)</td>
<td>(2 protocols)</td>
<td>✔️</td>
</tr>
</tbody>
</table>
IoTrim

IoT devices to protect
Companion App
IoTrim List Server
Home router running IoTrim software
What’s Next?

Privacy Preserving IoT Security Management

• Real industrial gateway
• Medical IoT Devices
• Real-world trial

Mitigation

• Real deployment and evaluation
• Third party certification

Privacy and Security Label/Certification

• Privacy and security by default
GET INTO IOT THEY SAID

IT WILL BE FUN THEY SAID
Follow us
Twitter: @iotrim @ammandalari
https://youtu.be/mMAH5UhEfOQ
https://youtu.be/P9AyJsMnX88
annamandalari.com