Benchmarking IoT Devices
Enhancing Privacy and Security in a Connected World

Anna Maria Mandalari
Why were we interested in this?

- They can (by definition) access the Internet and therefore may expose private information.
- 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).
- 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.
210 devices in different countries
Design of Experiments

>200k 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

<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.
Methodology

Internet Access Point Server

Analysis Scripts
Network Traffic Capture
Trigger Scripts

Linear TV
FAST TV
OTT
External Devices
Screen Casting

Network Traffic Capture

LOGGED IN - OPTED IN
Login
Opt-Out
Network Traffic Capture

LOGGED OUT - OPTED IN
Logout
Network Traffic Capture

LOGGED IN - OPTED OUT
Logout
Network Traffic Capture

LOGGED OUT - OPTED OUT
Network Traffic Capture

Comparison

Unsaved changes. Click here to save.

Share

LIn-OIn
LOut-OIn
LIn-OOut
LOut-OOut

View
Grid
Page View
Background
Background Color
Sketch
Options
Connection Arrows
Connection Points
Guides
Paper Size
A4 (210 mm x 297 mm)
Edit Data...
Clear Default Style
Change...

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
BENCHMARKING IOT PROTECTION SYSTEMS: 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).
Testbed

- **ISP / Internet**
- **Gateway**
- **LAN**
- **Safeguard**
- **IoT-LAN**
- **IoT Bridge**
- **L2 Bridge**

- **Android Phone**
- **NAT**

- **IoT Devices**
- **Packet capture and threat simulation**
- **Safeguard notifications and threat detection**
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 ≥ 1): The safeguard can detect the threat
- No: The safeguard cannot detect the threat

End (d=0)
### Evaluation of Threat Detection Capability

<table>
<thead>
<tr>
<th>Threat</th>
<th>Avira</th>
<th>Bitdefender</th>
<th>F-Secure</th>
<th>Fingbox</th>
<th>Firewala</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>✗</td>
<td>✓ (30s)</td>
<td>-</td>
<td>✗</td>
<td>✓ (30s)</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
</tr>
<tr>
<td>Weak Password</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>-</td>
<td>✗</td>
<td></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>-</td>
<td>-</td>
</tr>
<tr>
<td>SYN Flooding</td>
<td>✗</td>
<td>✓ (30s)</td>
<td>✗</td>
<td>-</td>
<td>✓ (40s)</td>
<td>✗</td>
<td>X</td>
<td>✗</td>
</tr>
<tr>
<td>UDP Flooding</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>DNS Flooding</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>HTTP Flooding</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>IP Fragmented Flood</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Port Scanning</td>
<td>✓ (45s)</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
<td>-</td>
<td>X</td>
<td>✓ (30s)</td>
</tr>
<tr>
<td>OS Scanning</td>
<td>✓ (45s)</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Malicious Destinations</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>-</td>
<td>✓</td>
<td>X</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>PII Exposure</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Unencrypted Traffic</td>
<td>✗</td>
<td>✗</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DNS over HTTPS</td>
<td>✗</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td></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.

**Time consistency**
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

IoTrimmer

Essential traffic

Goal 3: mitigation

Generalizable

Self adaptive

Accurate IoT blocker
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 port</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>
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)

- **Response Check**
  - yes → **SUCCESSFUL**
  - no → **FAILED**

- **Protocol Check**
  - yes → **FAILED**
  - no → **FAILED**

- **Any regular responses?**
  - yes → **FAILED**
  - no → **SUCCESSFUL**
Using ML for inferring IoT behavior

1. Use the `CheckLocalConnectivity` script to verify if the device leverages the local network.
2. If no local traffic is captured, proceed. If yes, continue with the next step.
3. Sniff the traffic while the device is set in the `OBVERSE / REVERSE` state via the `TrainingModule` 5 times.
4. Train ML models via the `TrainingModule`.
5. Sniff the traffic while the device is set in the `OBVERSE` state via the `AttackModule` and then set it in the `REVERSE` state.
6. Restart the scenario if no. If yes, proceed to the next step.
7. Restart the device via the `RestartDevice` script 50 times.
8. Perform the replay attack via the `AttackModule` and then invoke the `DetectionModule` with j=3.
## Results

**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>Yeelight lightstrip</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Yeelight bulb</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wiz lightbulb</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>
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
- Shared Database privacy and security vulnerabilities of IoT
Follow us
Twitter: @iotrim @ammandalari
https://www.youtube.com/watch?v=0fg0acuRbUA
annamandalari.com