Strengthening the IoT Ecosystem

Privacy Preserving IoT Security Management

Anna Maria Mandalari

UCL Imperial College London

Northeastern University

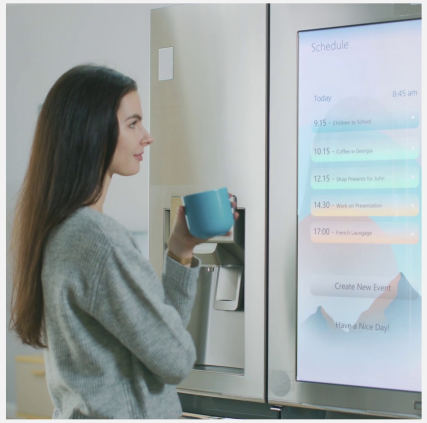
PETRAS EPSRC Pioneering research and skills NSF

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

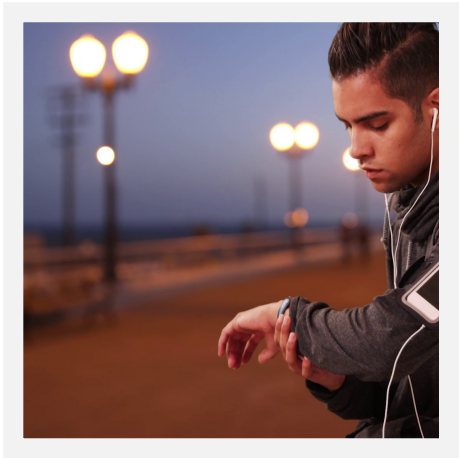
User Frustration

IoT devices privacy/security is hard to control

Hard to protect users from IoT threats

IOT PROTECTION SYSTEMS: SAFEGUARDS

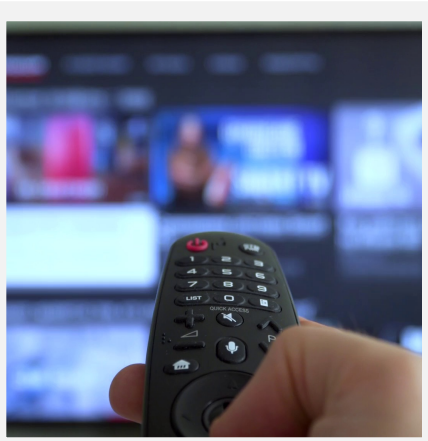
Why Were We Interested in This?



Control

Device detection

Intelligent profiles

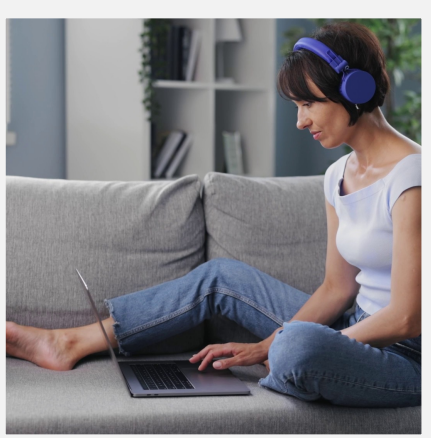


Security

Vulnerability Assessment

Brute Force Protection

Anomaly Detection



Privacy

Content filtering

Network Intrusion Prevention

- 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

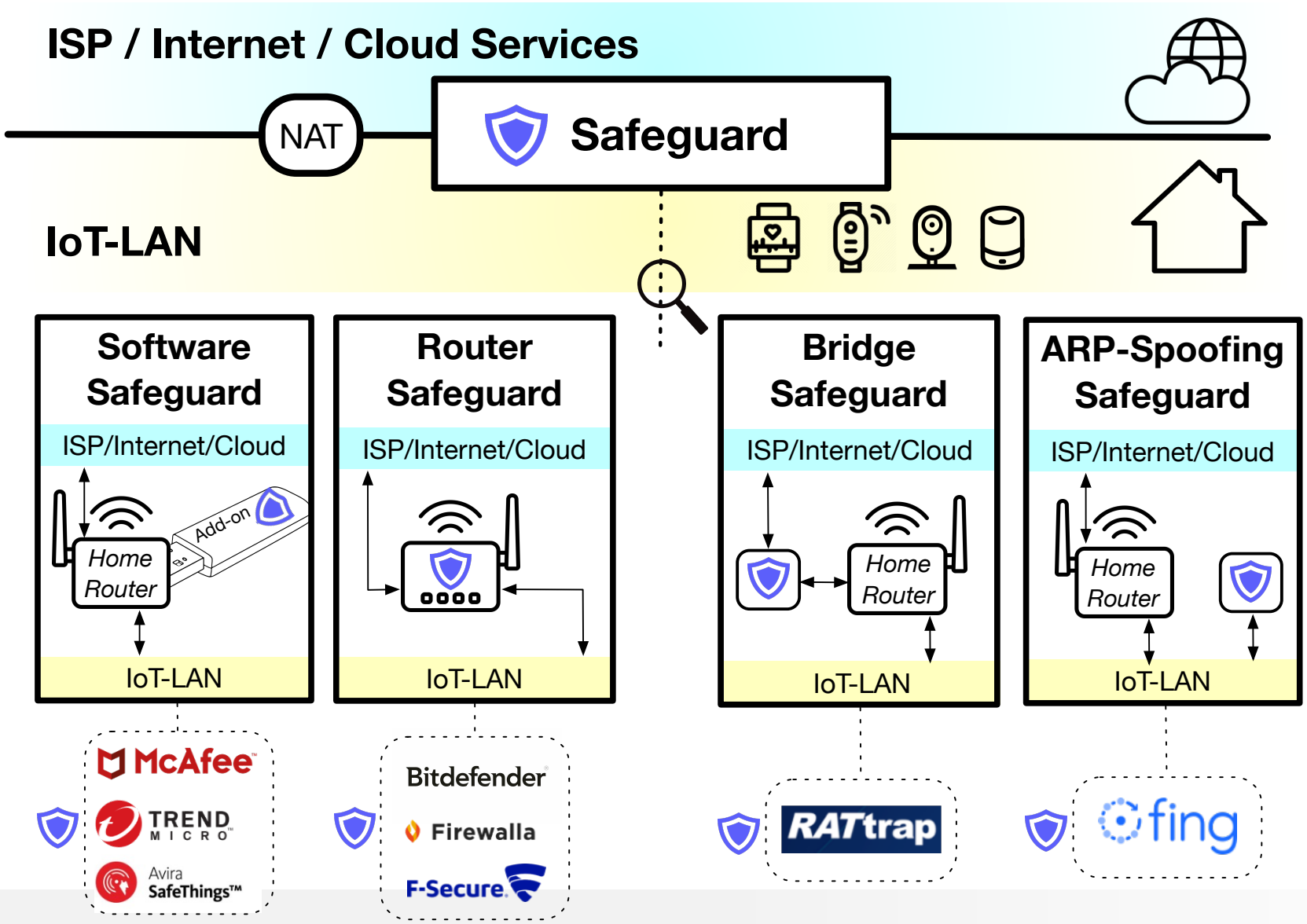
- Closed systems
- Blackbox approach

Difficult to perform IoT experiments and generalize

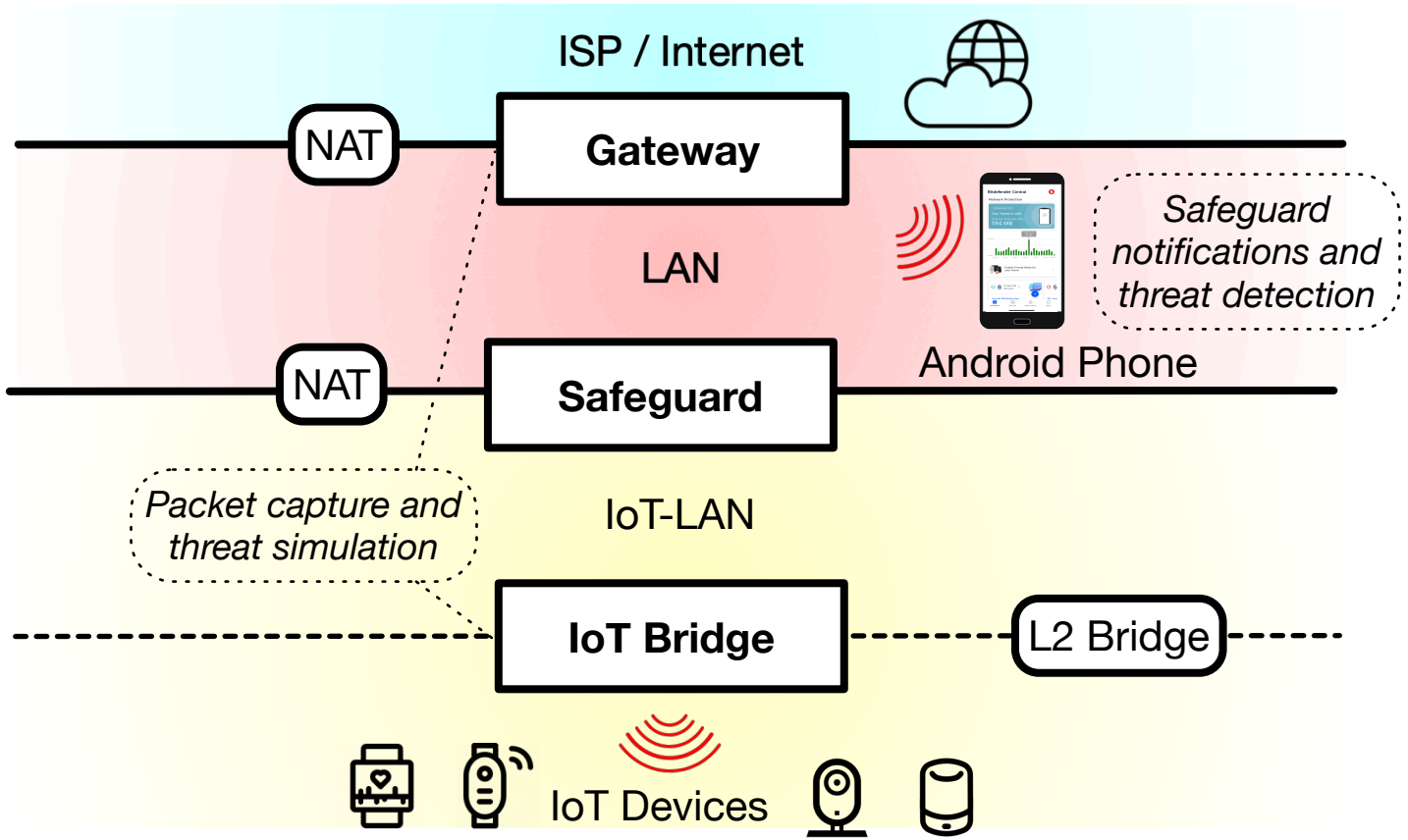
- Lack of automation and emulation tools
- Lack of standard testbed

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

Selecting IoT Safeguards



Testbed

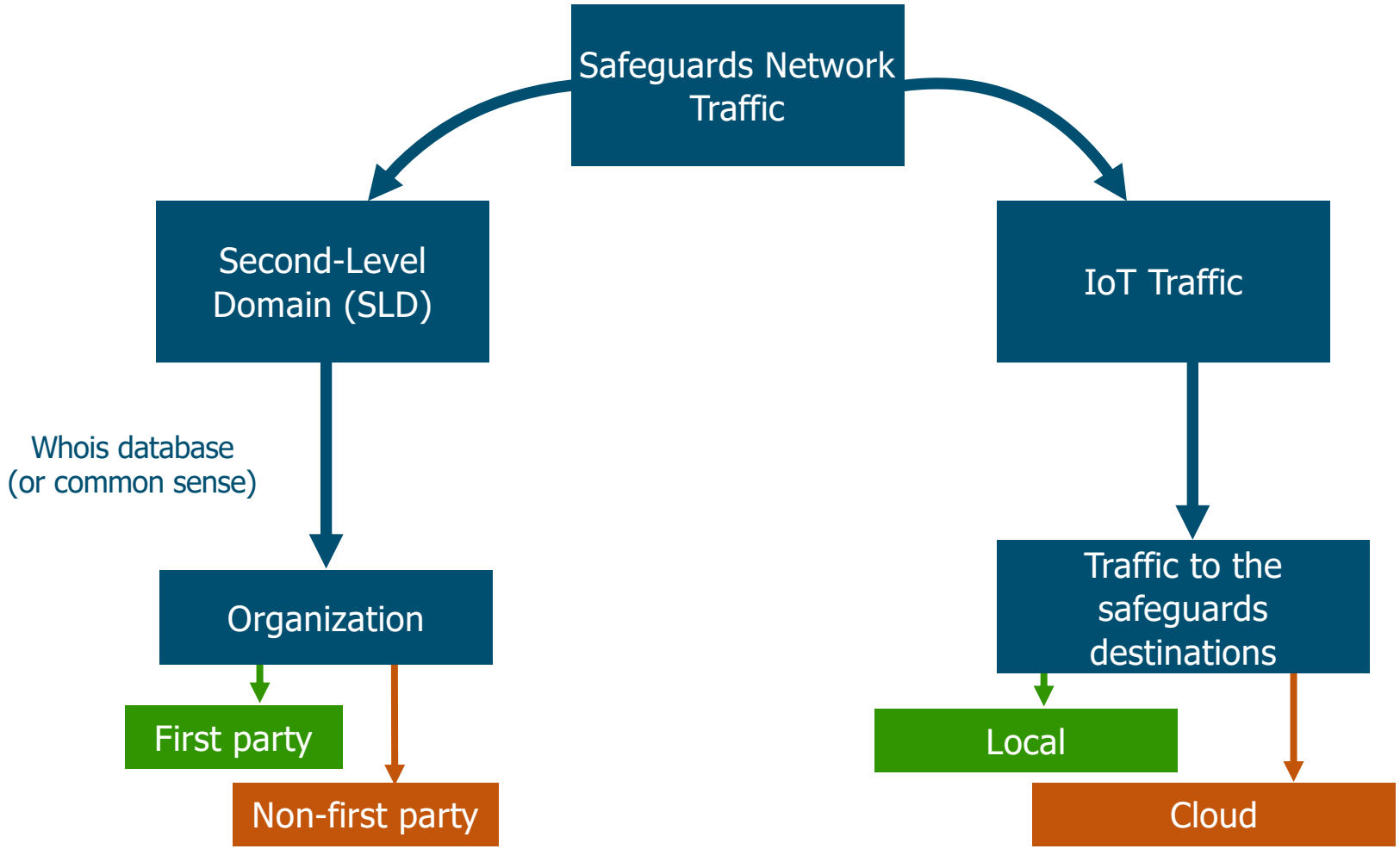

ISP / Internet
NAT
Gateway
LAN
Safeguard notifications and threat detection
Android Phone
NAT
Safeguard
Packet capture and threat simulation
IoT-LAN
IoT Bridge
L2 Bridge
IoT Devices

Research Questions

- **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

IoT Safeguards

Processing Locality & Party Characterization

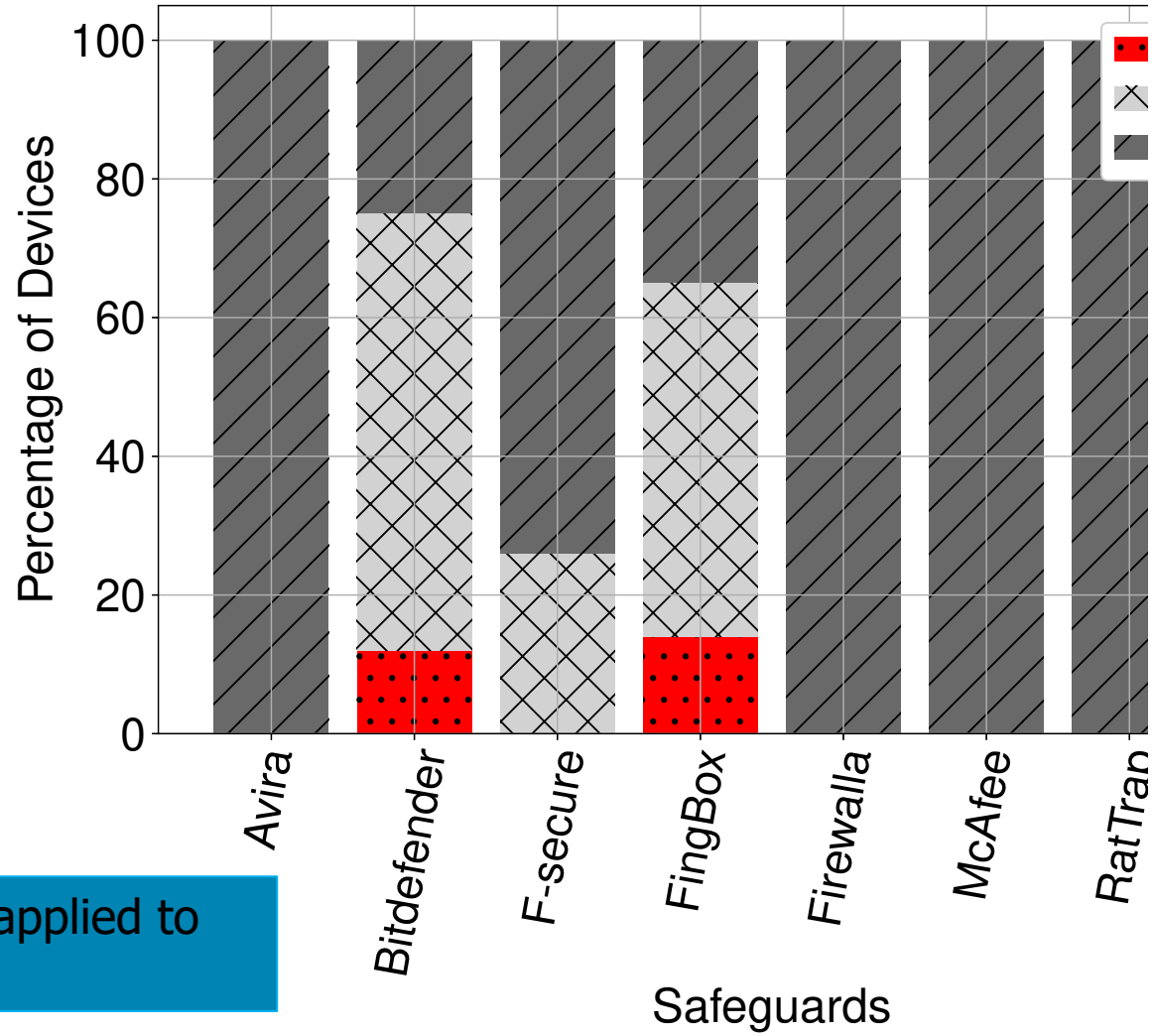


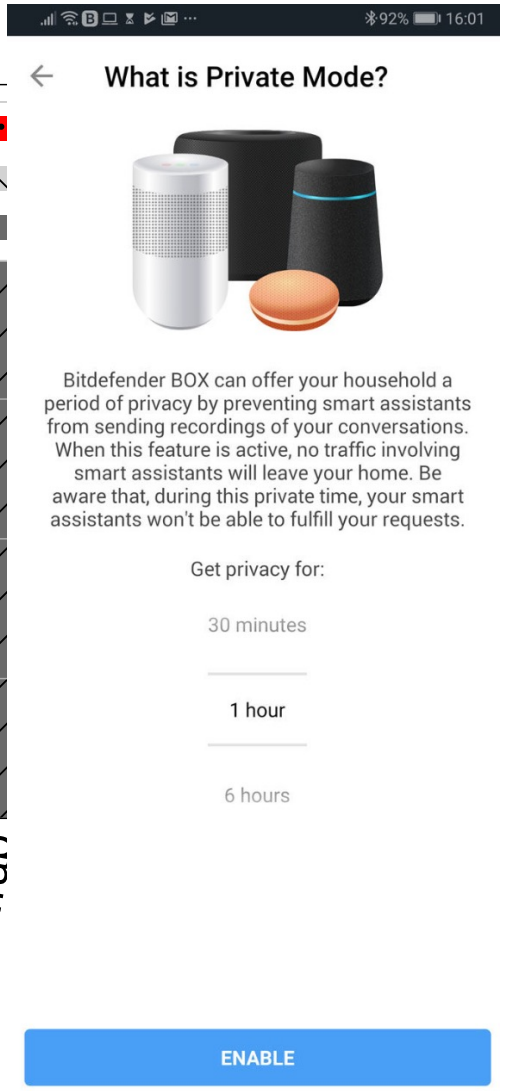
Processing Locality & Party Analysis

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

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

Take away: only a small 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

IoT Safeguards

Testing Threat Detection Capability

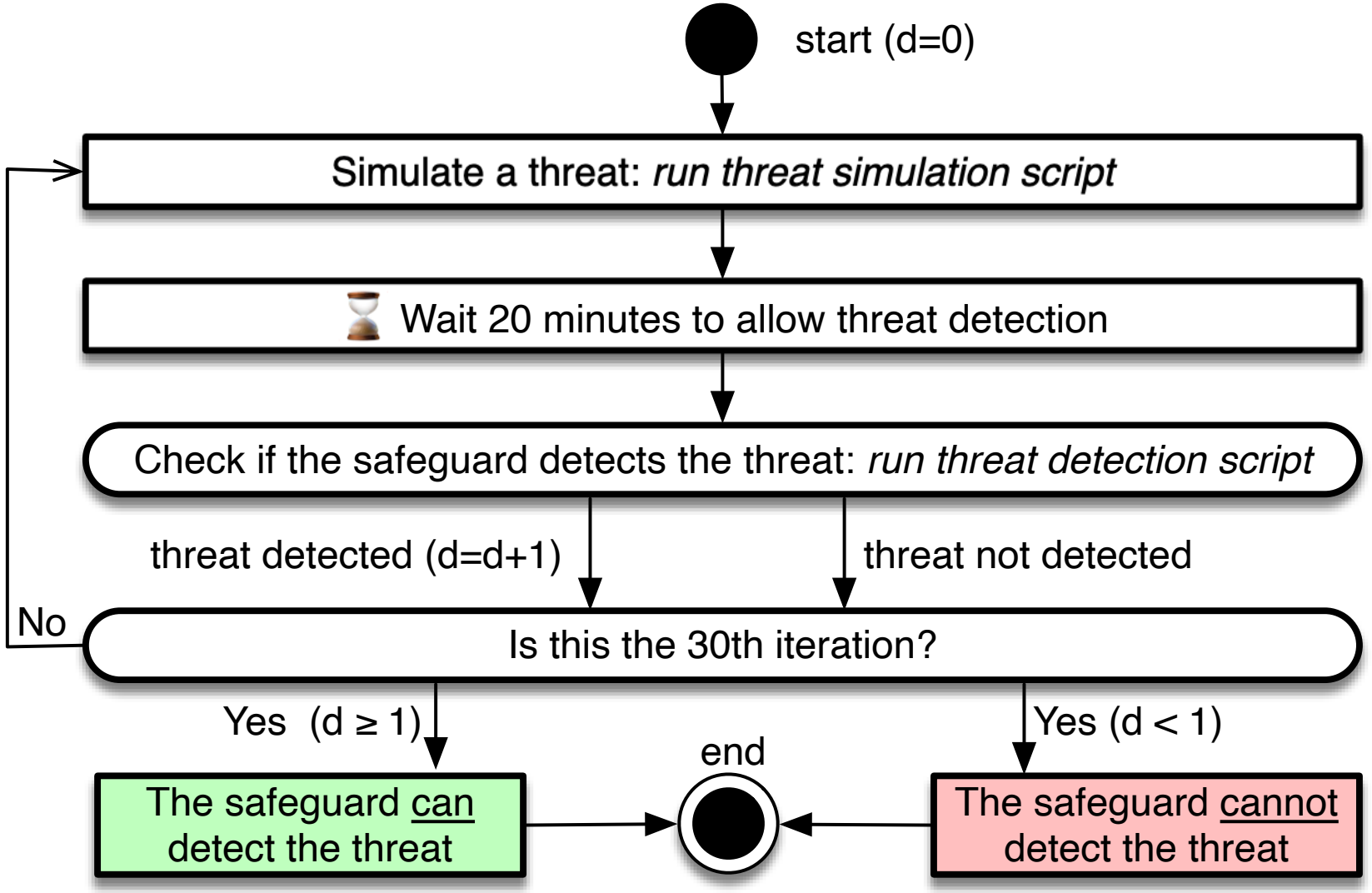
- Security

Threats
Anomalous behavior
Open Port
Weak Password
Device Quarantine
DoS attacks
Port/OS Scanning
Malicious Destinations

- Privacy

Threats
PII Exposure
Unencrypted Traffic
DNS over HTTPS

Threat Detection Experiments



Evaluation of Threat Detection Capability

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

Time consistency

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.

Research Questions

- **Goal 3:** What are the side effects of the safeguards?
  - **Traffic overhead, overprotection, privacy implications**

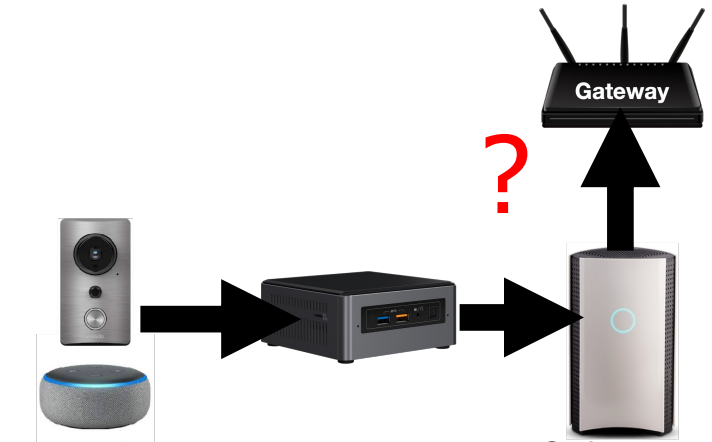
IoT Safeguards

Safeguard Side Effects

Overprotection

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

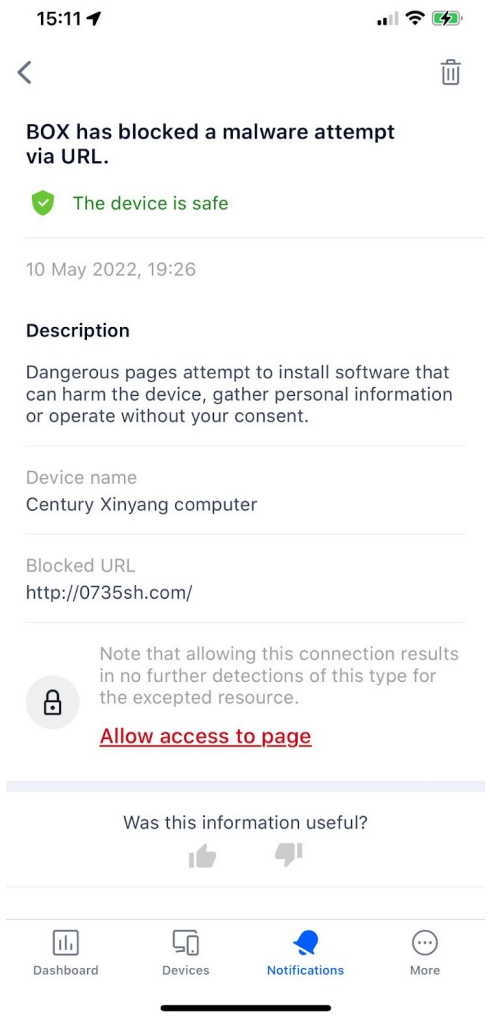
Network traffic overhead



Privacy Policy

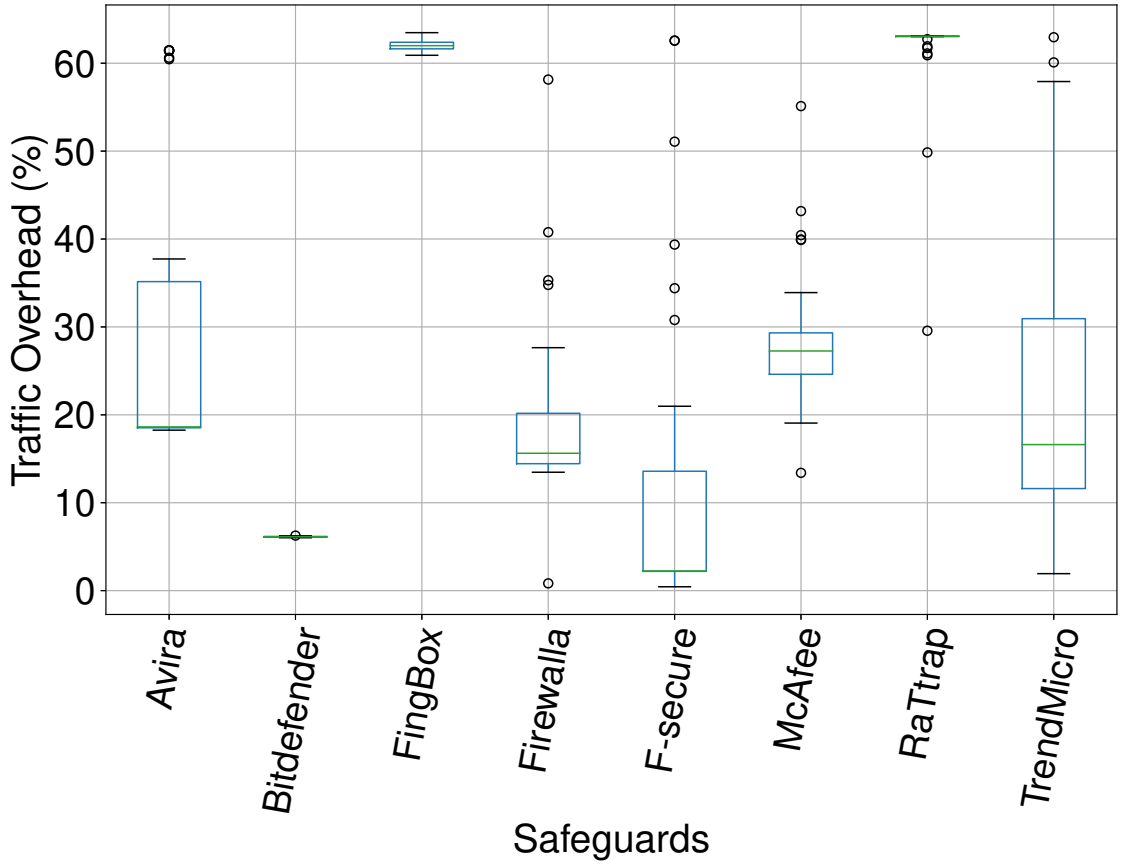
MANUALLY INSPECTING THE PRIVACY POLICY

Overprotection



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

Traffic Overhead



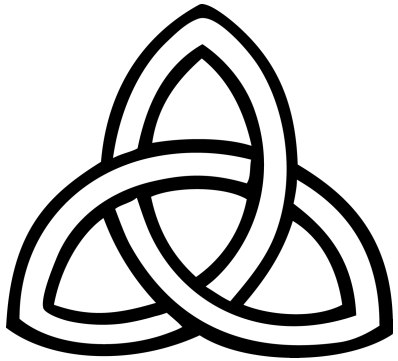
Take away: Some of the safeguards introduce significant traffic overhead. In general the overhead is never less than 10% of the traffic of the IoT devices.

Privacy Policy

Privacy Policy	Avira	Bitdefender	F-Secure	Fingbox	Firewalla	McAfee	RaTtrap	TrendMicro
Anonymization	✓	✓ [pseudonymize]	X [ceasing subscription]	✓	X	X	X	X
Usageof Personal Data	✓	✓	✓	✓	✓	✓	✓	✓
Retention Period	In accordance with legal requirements	10 years	6 months	As long as necessary	Indefinitely	Subscription period	Subscription period	Ongoing legitimate business need
Third Party	SaaS vendor, Akamai. Mixpanel, Ivanti	Partners	Partners	Partners	X	Partners	Partners	Partners

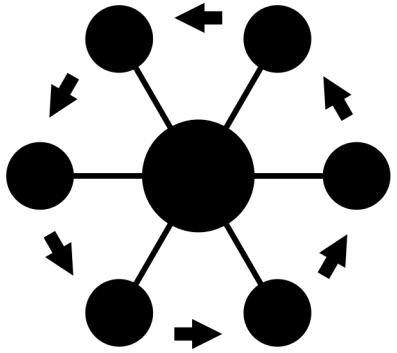
Take away: Most user information is shared with third-party entities, sometimes without anonymization. Sharing data outside user's privacy jurisdiction.

Strengthening the IoT Ecosystem



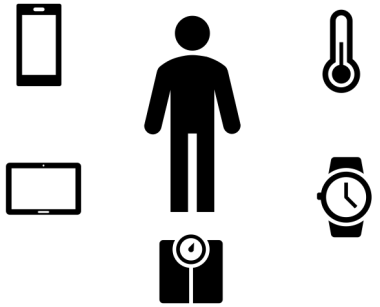
Trust

- 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

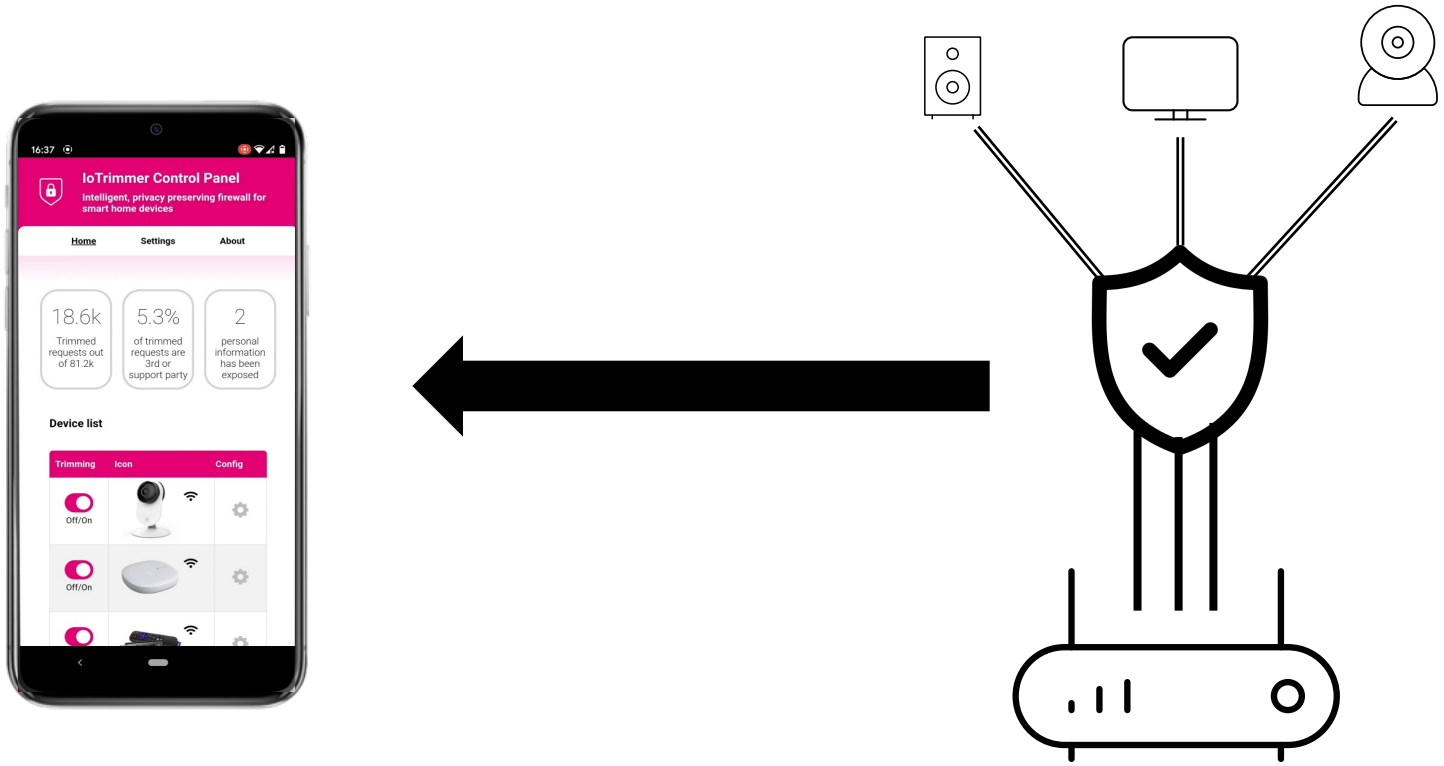


Awareness, Authentication & Management

- Usable monitors for IoT
- Context-aware privacy
- Personalised privacy

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



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

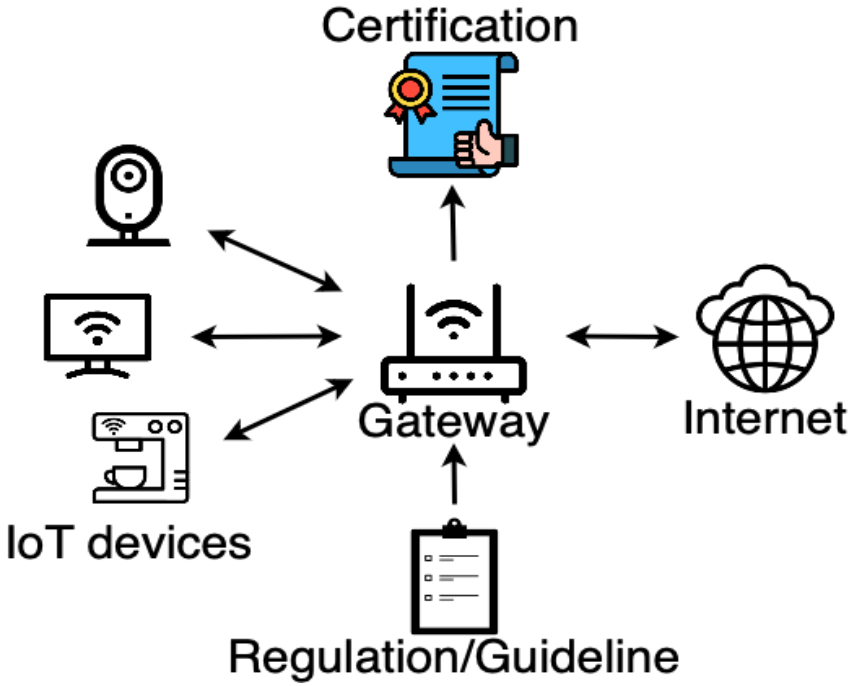
- In 2023 the **Cyber Resilience Act** (in EU) and the **US Cyber Trust Mark** (in US) make further step towards a certification program of smart devices

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

- **Should we trust vendors?**

Methodology

Select security guidelines and privacy regulations → Turn them into metrics → Define experiments to test the extracted metrics on IoT devices → Produce a certification label for the tested device



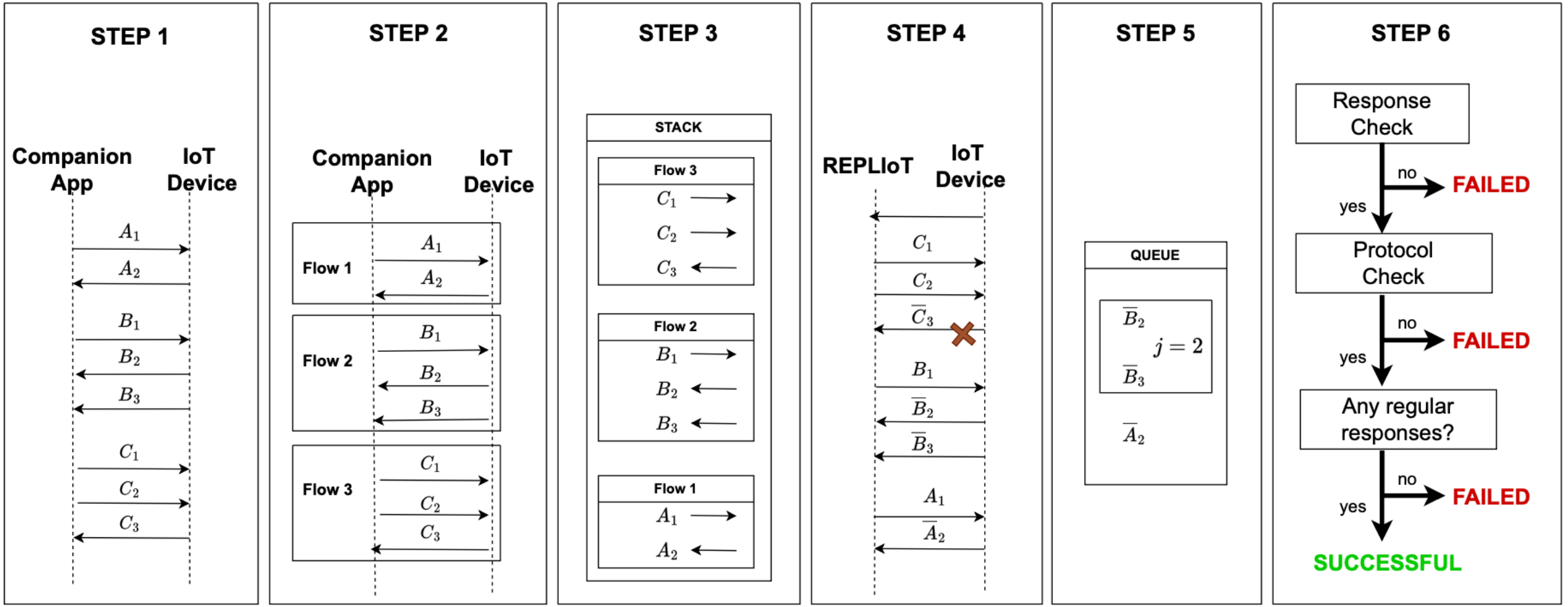
Results

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

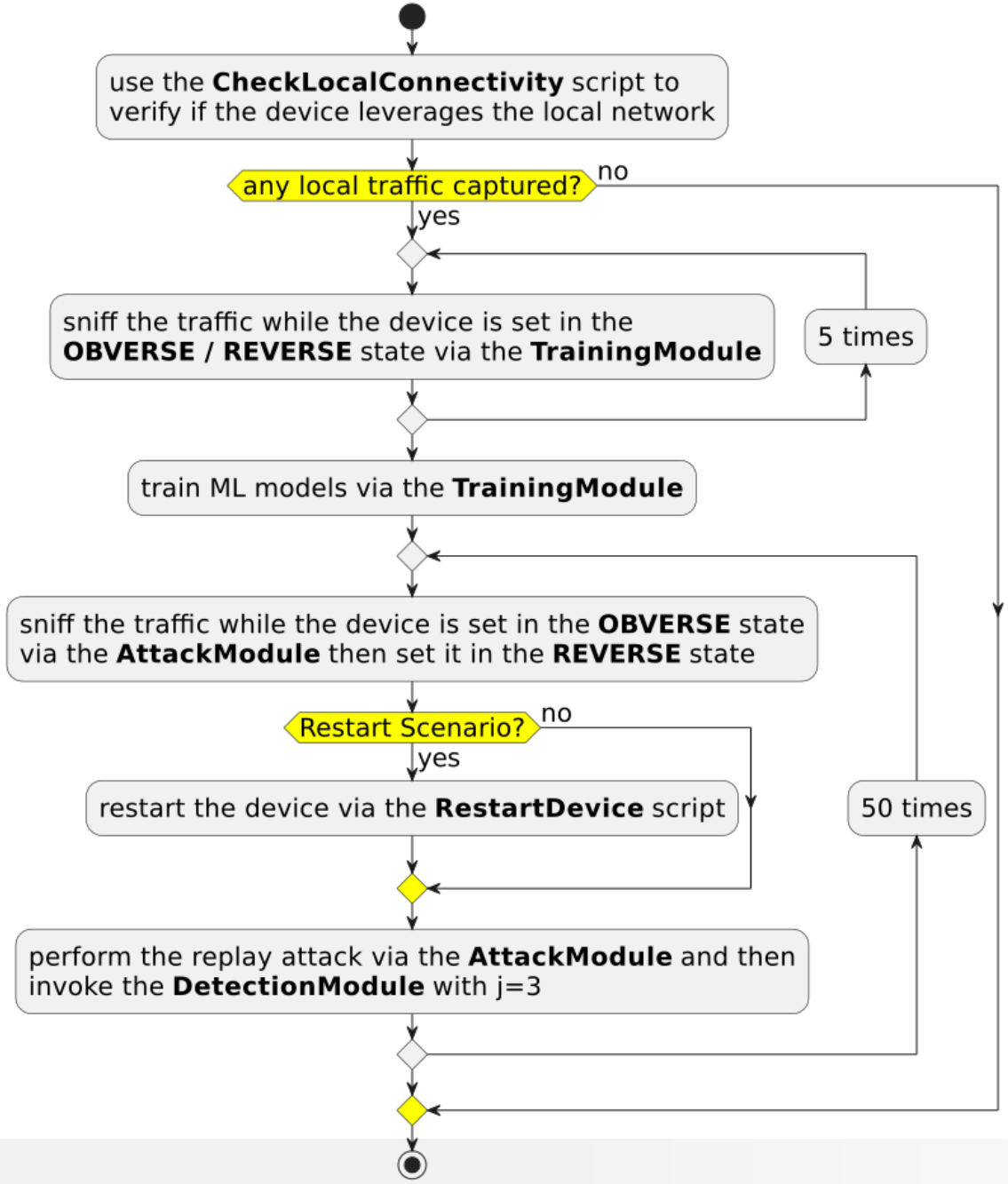
Is Your Kettle Smarter Than a Hacker?

- **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



Methodology

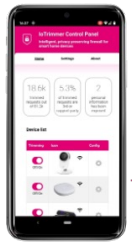


Results

REPLAY ATTACK RESULTS. ✓ INDICATES WHETHER THE REPLAY ATTACK IS SUCCESSFUL OR NOT (X).

Device (*Tested via APIs)	Non-Restart Scenario	Restart Scenario
Yeeligth lightstrip	✓	✓
Yeelight bulb	✓	✓
Wiz ligthbulb	✓	✓
Lifx bulb	✓	✓
Lepro bulb	✓	✓
Govee lightstrip *	✓	✓
Nanoleaf triangle *	✓	✓
Tapo smartplug	✓	X
Meross smartplug	✓	✓
WeeKett Kettle	✓	✓
Eufy robovac 30C	✓	✓
OKP vacuum	✓	✓
iRobot roomba i7	X	X
Sonos Speaker *	✓	✓
Bose Speaker *	✓	✓
Wyze cam pan	X	X
Vtech baby monitor	X	X
Boyfun Baby monitor	X	X
Furbo camera	X	X
Meross Garage Opener	✓	✓

IoTrim

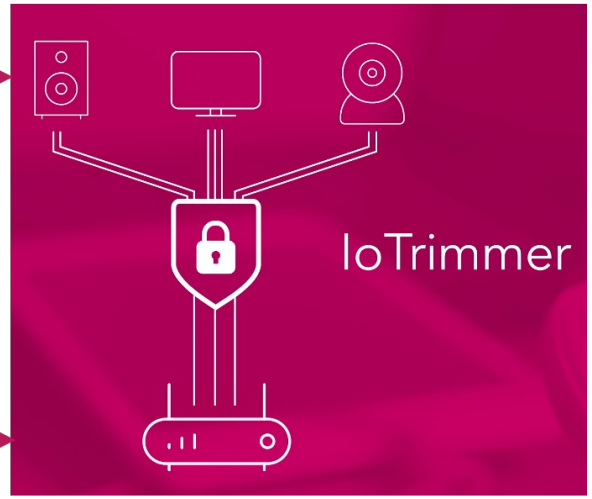


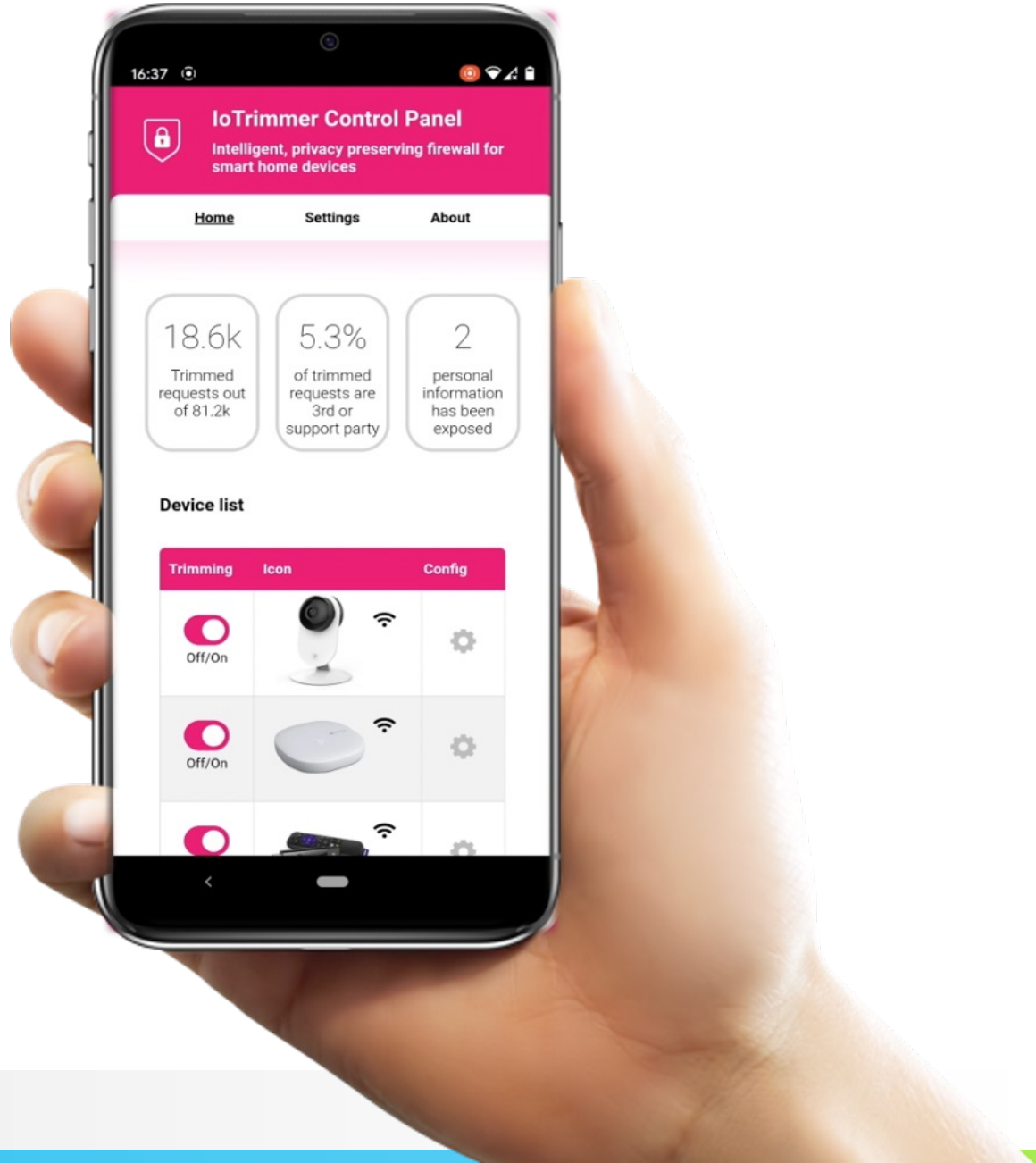
IoT devices to protect

Companion App

IoTrim List Server

Home router running IoTrim software



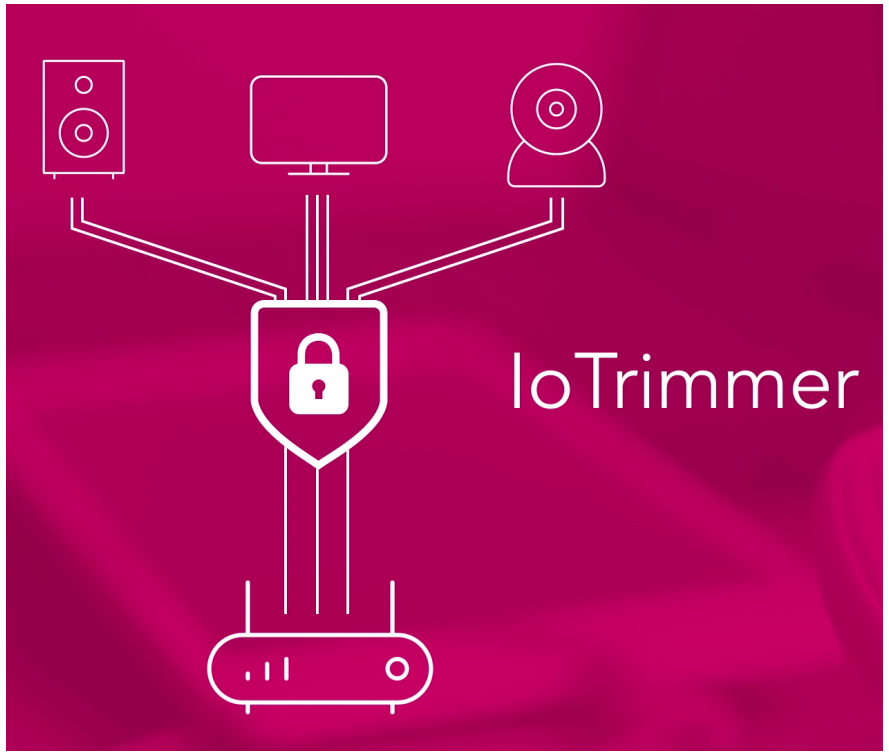


Conclusion

- Quantitative approach for auditing IoT safeguards, as well as analyzing their data-collection and sharing practices
- Scalable methodology for evaluating the effectiveness of the safeguards against known IoT and network security attacks and threats
- Often they do not provide advertised protection; their data-sharing practices might also introduce potential privacy threats to their users
- All our software and data are open source and available for download

Impact:

- **Responsible Disclosure:** Working with vendors to encourage better protection efforts
- Testbed/analysis framework and data are publicly available



Follow us

Twitter: @iotrim @ammandalari

https://youtu.be/mMAH5UhEfxQ

https://youtu.be/P9AyJsMnX88

annamandalari.com