Policy Certification and Verification for Cybersecurity in the IoT

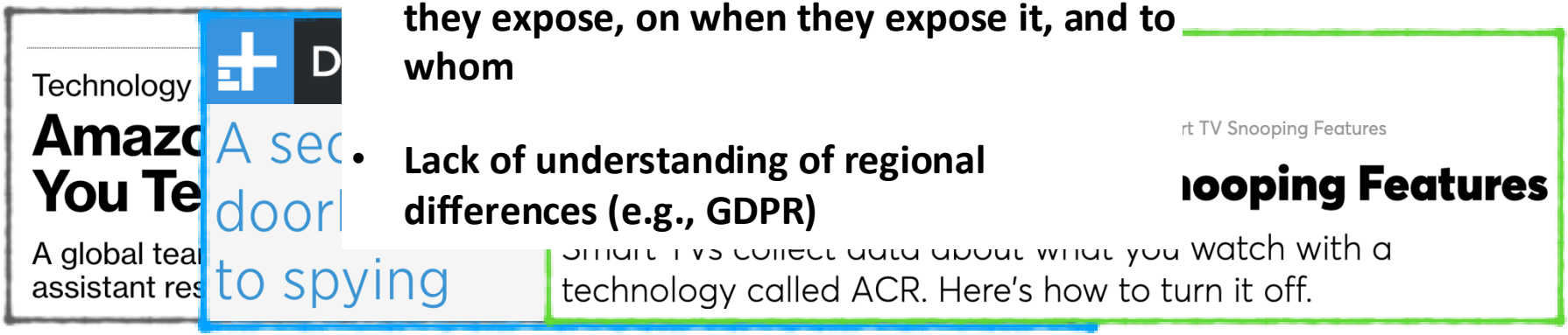
Anna Maria Mandalari

Why were we interested in this?

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

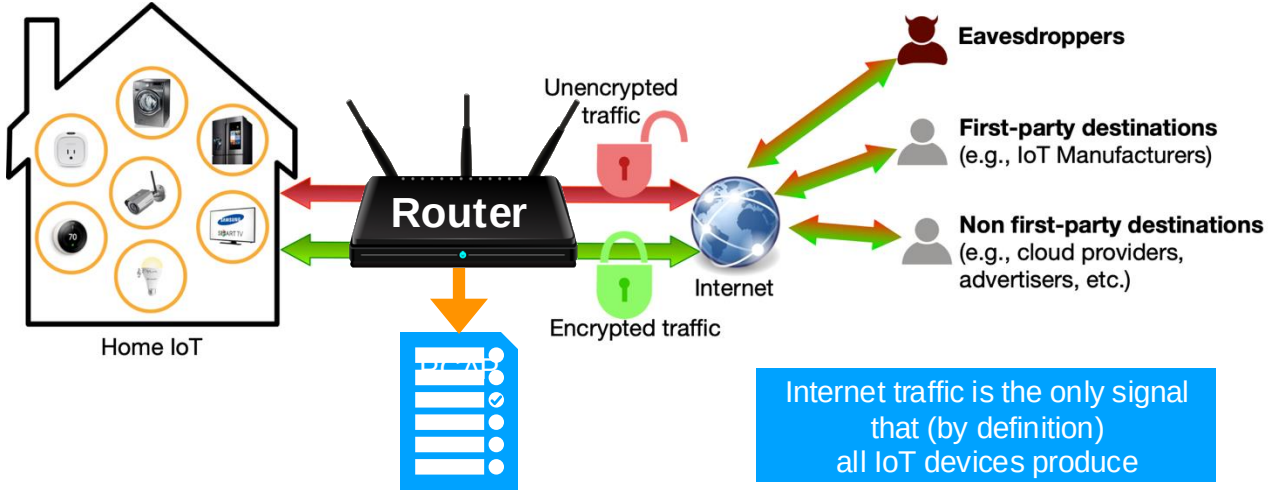
- They can (by definition) access the Internet and therefore may expose private information
- Lack of understanding on what information they expose, on when they expose it, and to whom
- Lack of understanding of regional differences (e.g., GDPR)

ey may know what
vatch (e.g., smart TVs)



210 devices in different countries

Data Collection Methodology



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

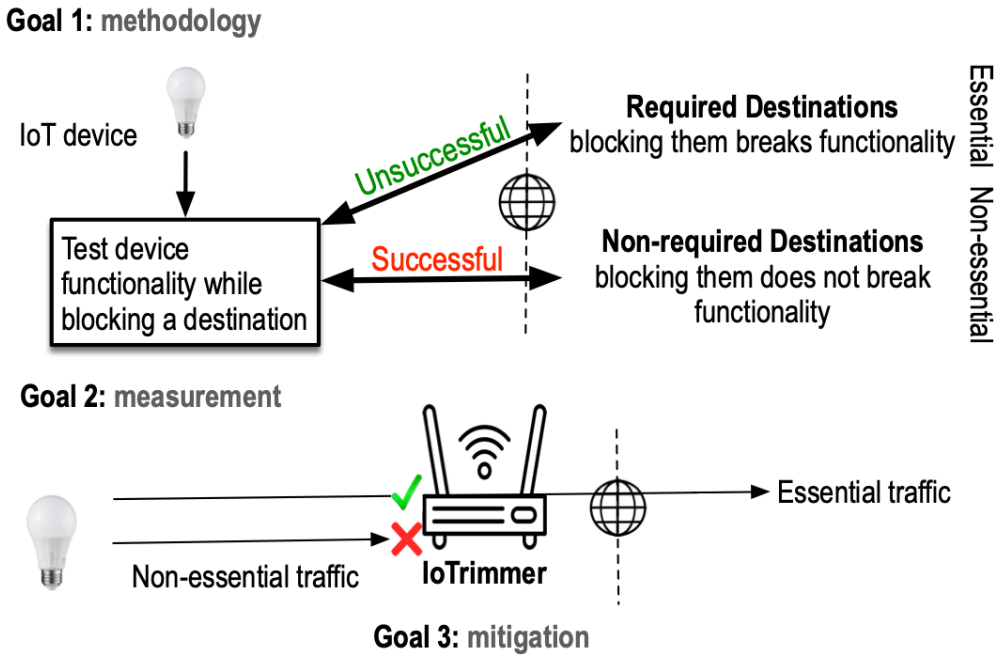
Motivation

- 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?

Solution at the Edge



/ Generalizable

/ Self adaptive

/ Accurate IoT blocker

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

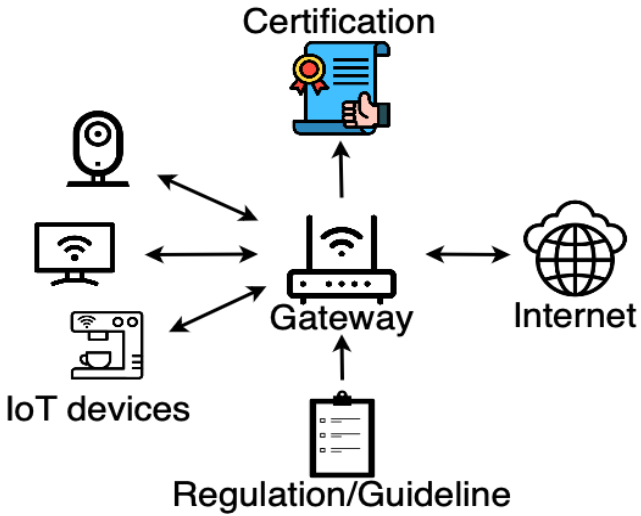
Privacy regulations** such as GDPR (in EU) and CCPA (in California)

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

***NOT mandatory**
****Mandatory**

Methodology

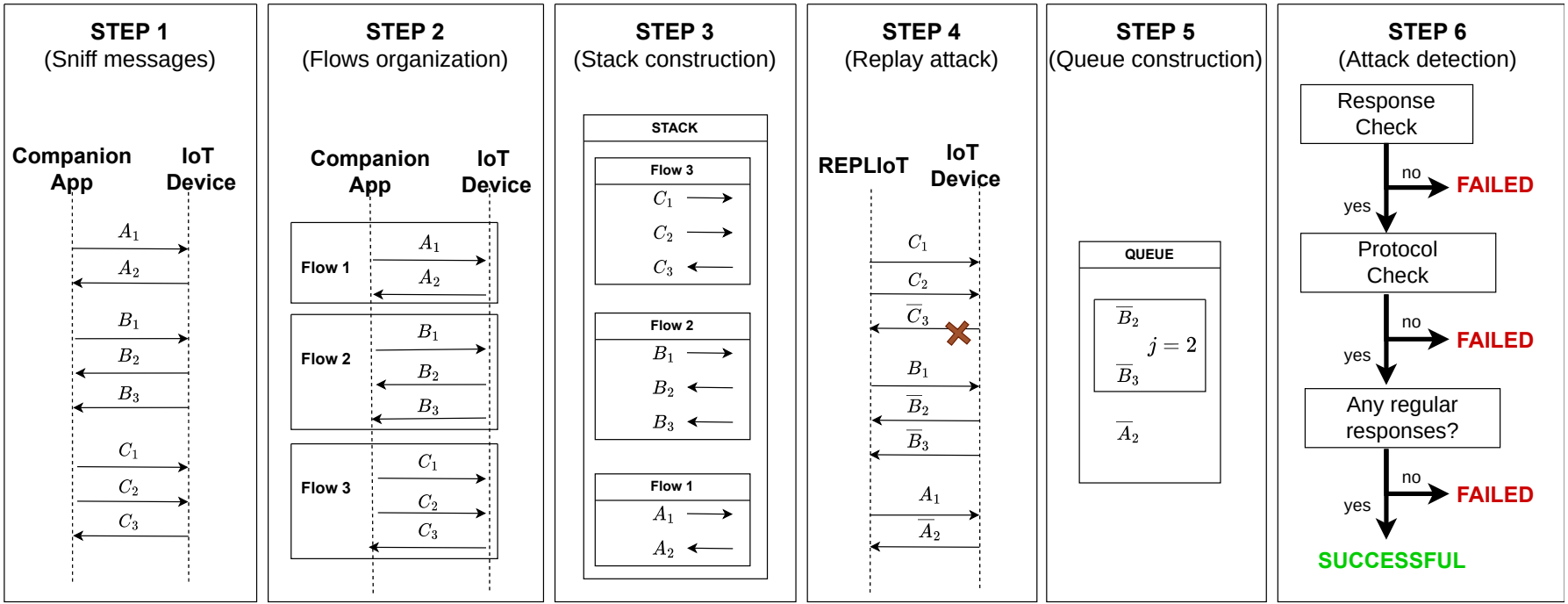
Select security guidelines and privacy regulations → Turn them into metrics → Define experiments to test the extracted metrics on IoT devices → Produce a certification label for the tested device



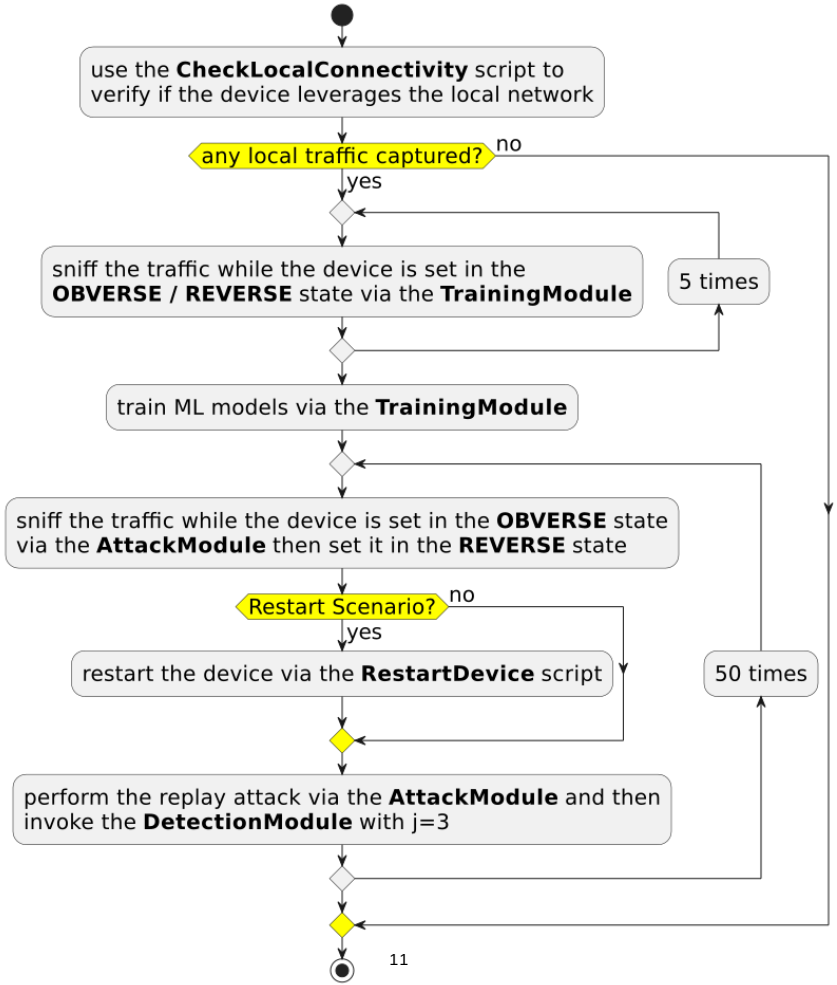
Results

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)	✓

Methodology



Using ML for inferring IoT behavior



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	✓	✓

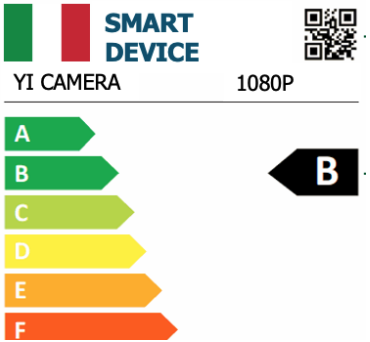
What's Next?

Privacy Preserving IoT Security Management

- Real industrial gateway
- Real-world trial

Mitigation

- Open source software
- Third party certification
- Manufactures Guidelines



Privacy and Security Label/Certification

- Privacy and security by default
- IETF/ETSI Standard

Our Team

Anna Maria Mandalari

Assistant Professor
University College London

Honorary Research
Fellow at Imperial College
London

Fabio Palmese

Senior Developer

Hamed Haddadi

Professor in Human-Centred Systems at Imperial College London

Mulini

Follow us:

@iotrim @ammandalari

mulini.eu