# Policy Certification and Verification for Cybersecurity in the IoT

Anna Maria Mandalari


UCL

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

# Agenda

01 **Problem: IoT Devices Expose Information Over the Internet**

Reasons you shouldn’t watch TV
Reasons you shouldn’t use smart medical devices.

02 **Privacy and Security Certification/Regulation**

EU Cyber Resilience Act (CRA)
GDPR

03 **IoT Automating Testing and Compliance**

IoTrim ++
Black box assessment

04 **Standards**

Standardization request
ETSI/CEN-CENELC WGs

05 **Gaps**

IoT Manufactures
SMEs

06 **Conclusion**

What’s next?

# Agenda

01 **Problem: IoT Devices Expose Information Over the Internet**

Reasons you shouldn't watch TV
Reasons you shouldn't use smart medical devices.

02 **Privacy and Security Certification/Regulation**

EU Cyber Resilience Act (CRA)
GDPR

03 **IoT Automating Testing and Compliance**

IoTrim ++
Black box assessment

04 **Standards**

Standardization request
ETSI/CEN-CENELC WGs

05 **Gaps**

IoT Manufactures
SMEs

06 **Conclusion**

What's next?

# 210 devices in different countries

01

# Reasons You Shouldn't Watch TV

# Motivation

I Still Know What You Watched
Privacy of the HbbTV Protocol in
Smart TV Landscape

Carlotta Tagliaro
TU Wien
Austria
carlotta@seclab.wien

Janus Varmarken*, Jad Al Aaraj, Rahmadi Trimananda, and Athina Markopoulou

**FingerprinTV: Fingerprinting Smart TV Apps**

**Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices**

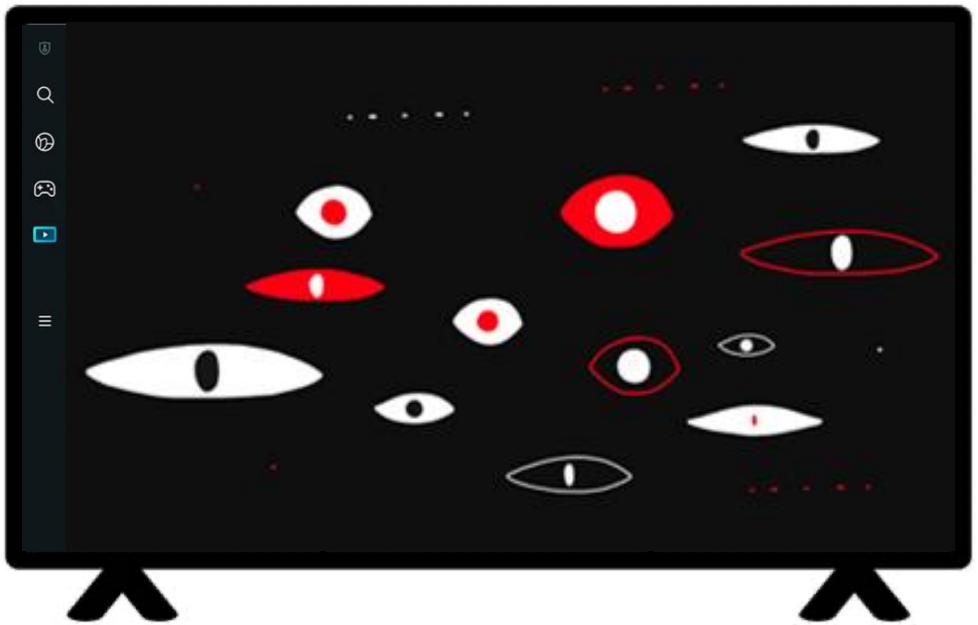
Hooman Mohajeri Moghaddam, Gunes Acar, Ben Burgess, Arunesh Mathur, Danny Yuxing Huang,
Nick Feamster*, Edward W. Felten, Prateek Mittal, Arvind Narayanan
Princeton University and University of Chicago*

Marcos Tileria* a

**Watch Over Your TV: A Security and Privacy Analysis of the Android TV Ecosystem**

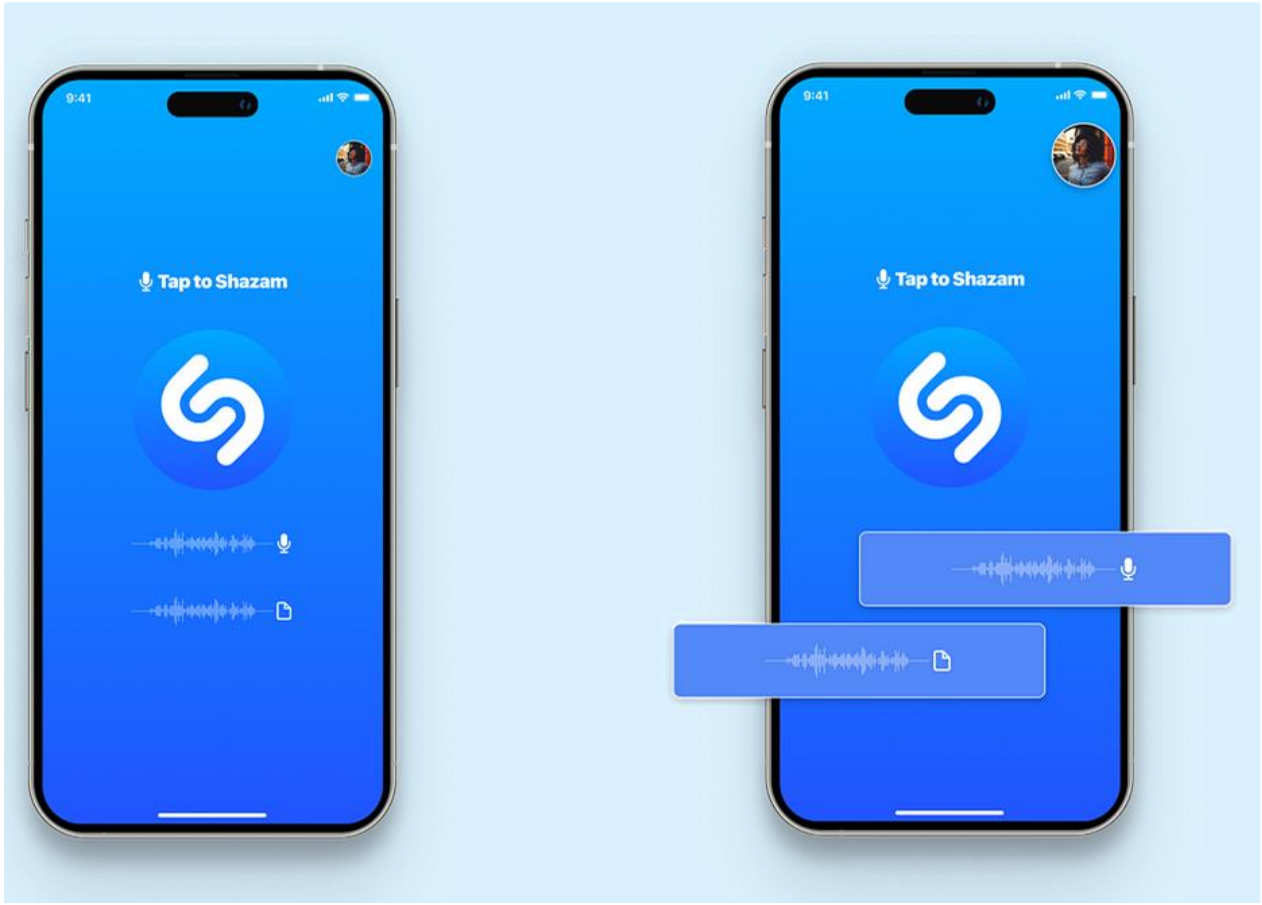
Janus Varmarken†*, Hieu Le†, Anastasia Shuba, Athina Markopoulou, and Zubair Shafiq

**The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking**

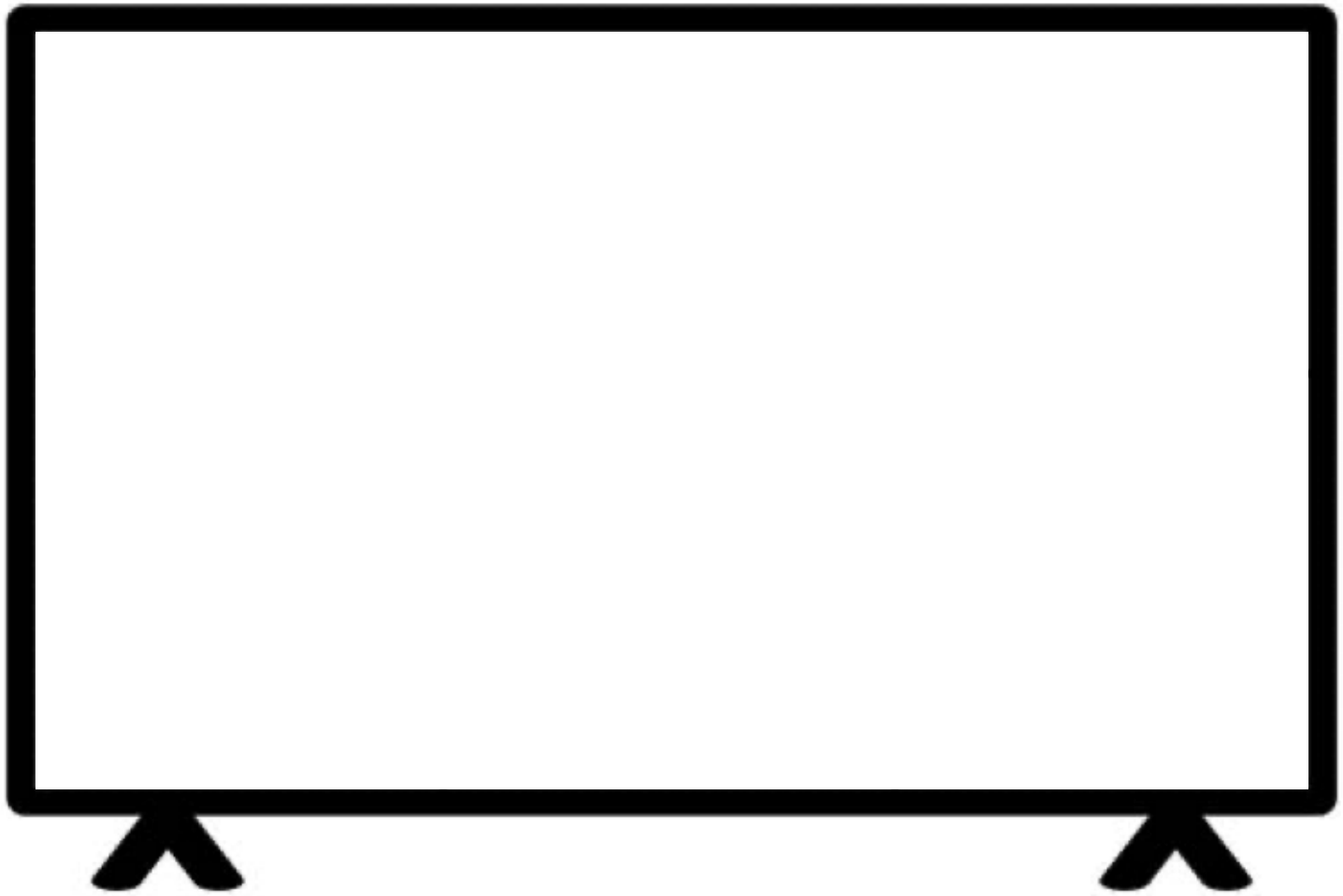



3P apps or services

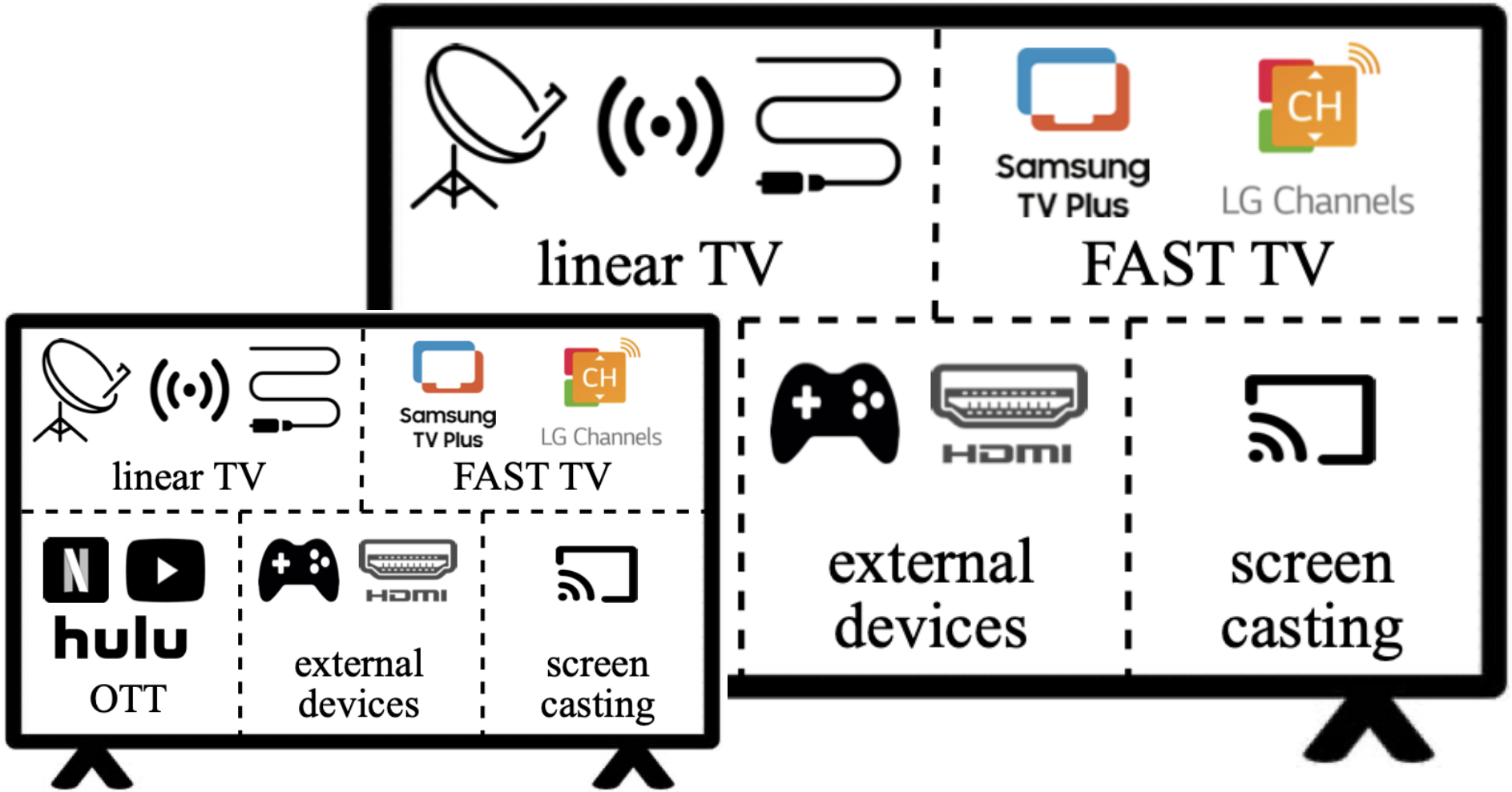
# ACR = OS-integrated Shazam-like technology



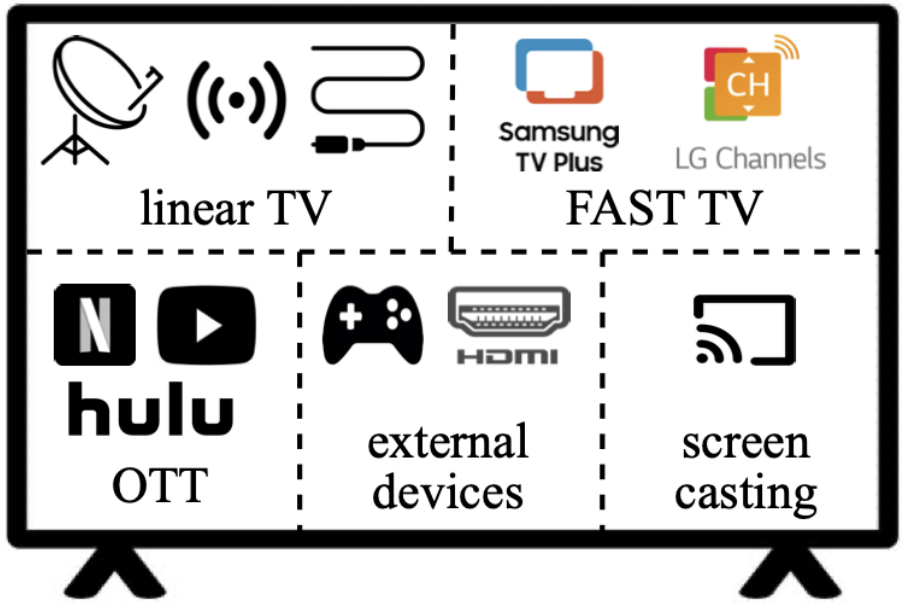

# Smart TV Functionalities



# Automatic Content Recognition (ACR)

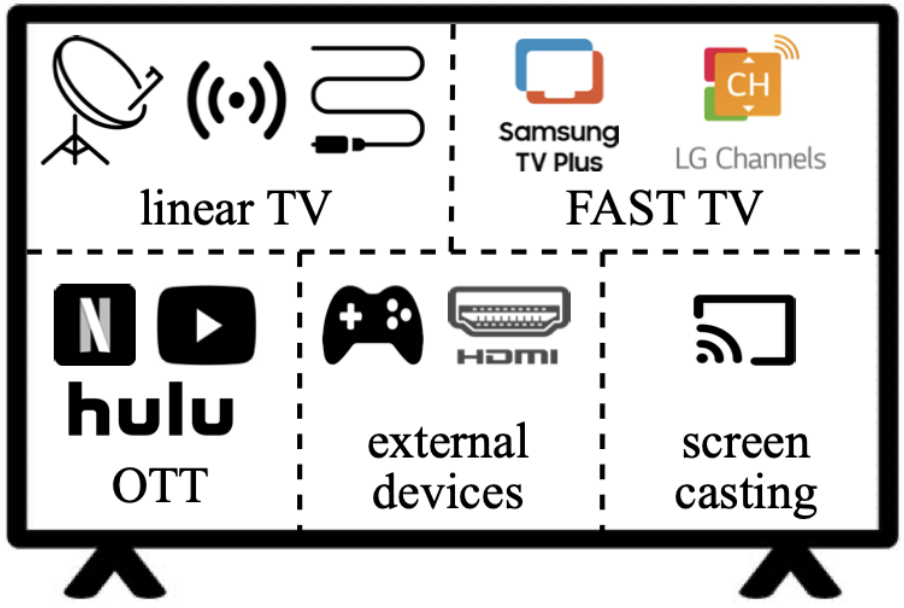


# ACR Client

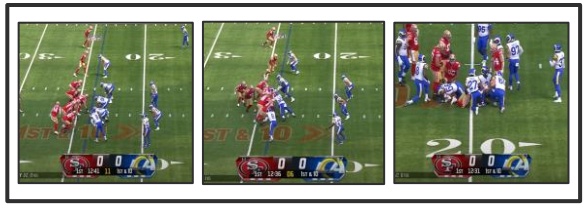

linear TV
Samsung TV Plus
LG Channels
FAST TV
hulu
OTT
HDMI
external devices
screen casting

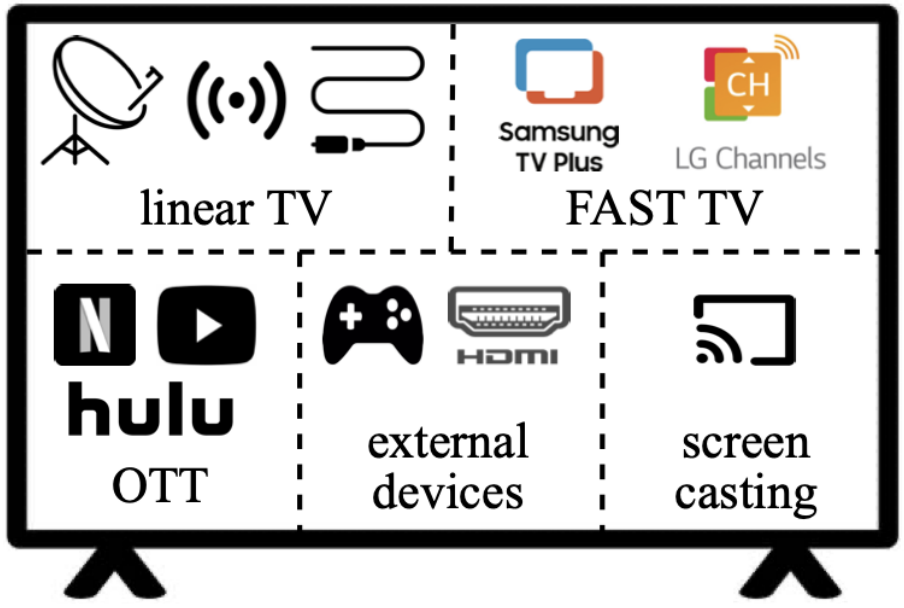

TV

## ACR Client


Samsung TV Plus
LG Channels
linear TV
FAST TV
hulu
OTT
HDMI
external devices
screen casting


Captured frames



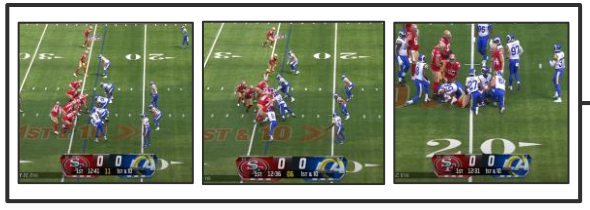


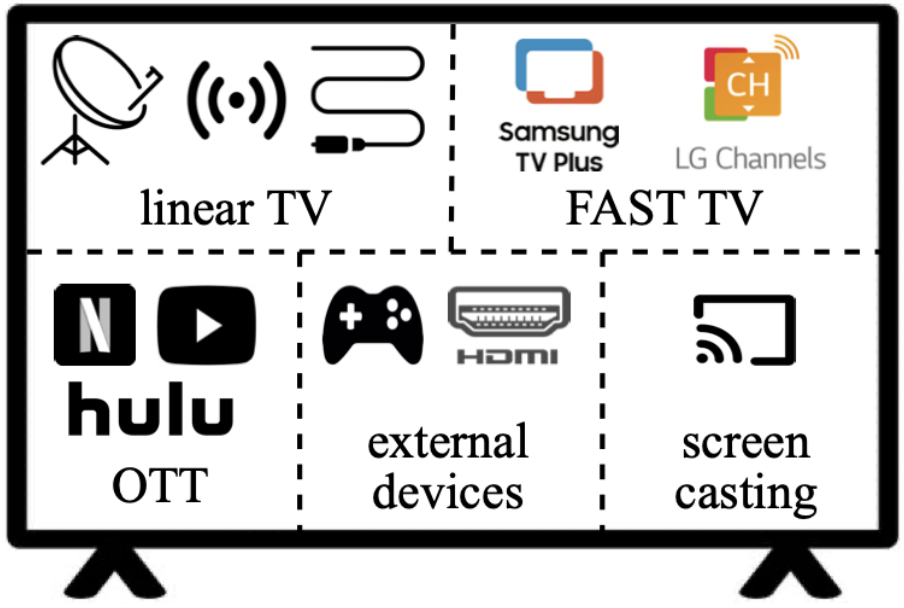

## ACR Client


Captured frames

Content fingerprint

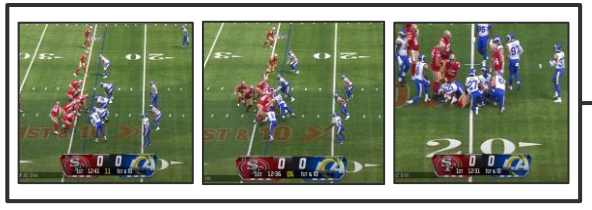
**ACR Client**



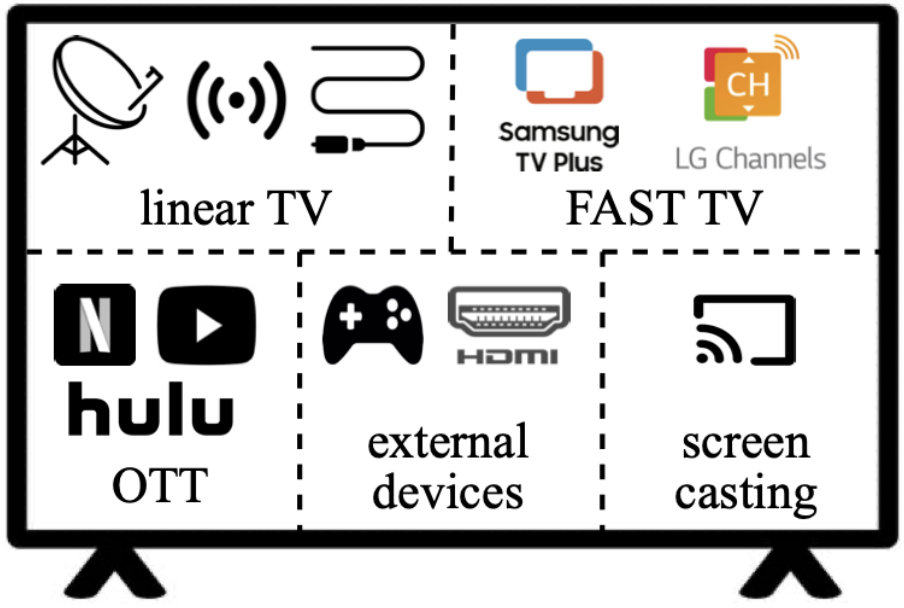



Captured frames

Content fingerprint

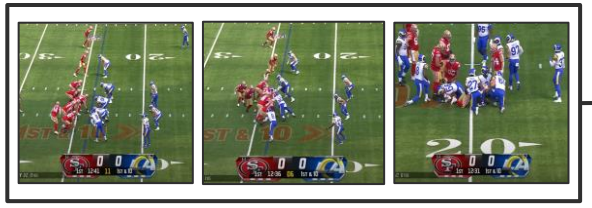


**ACR Client**




**ACR Server**

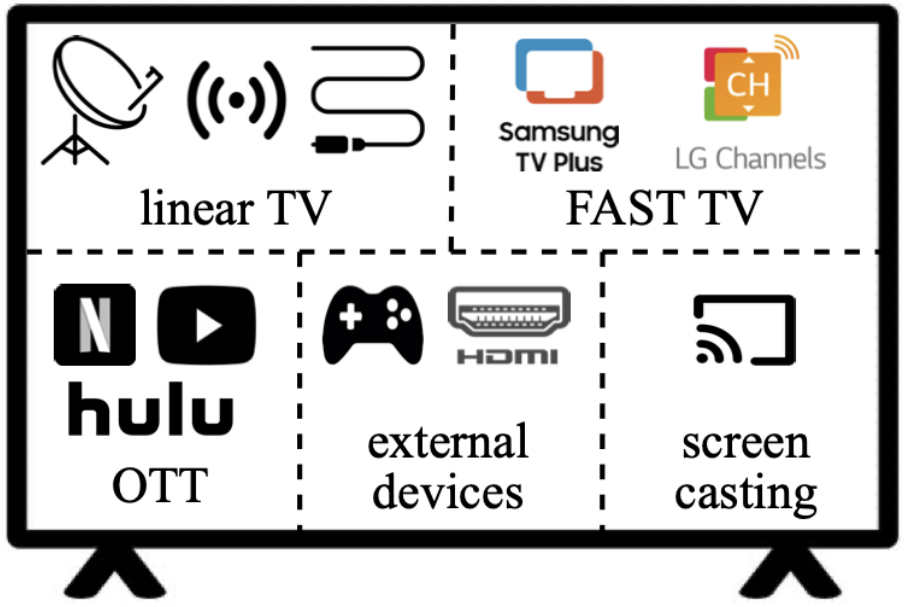

Captured frames



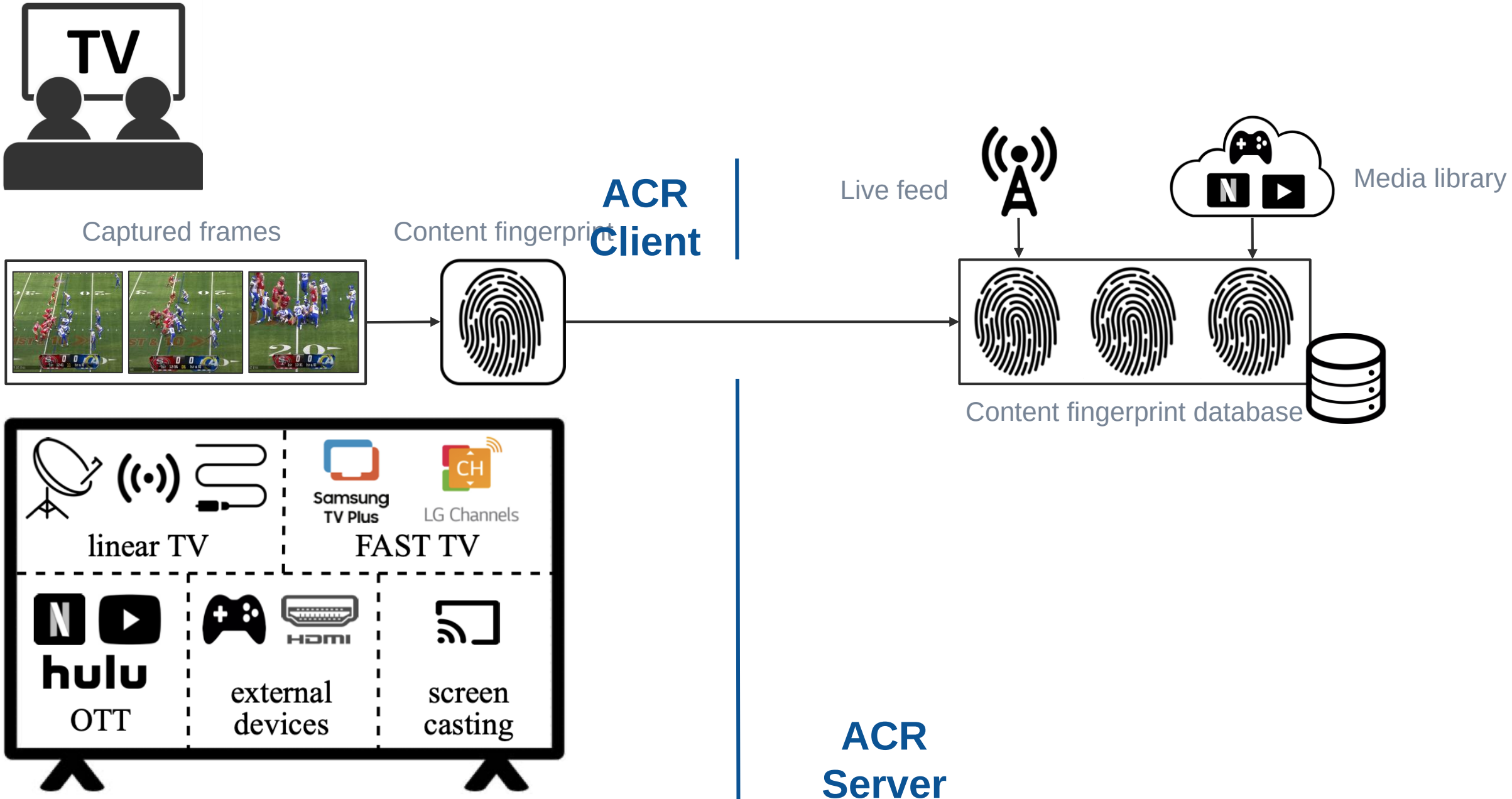
Content fingerprint

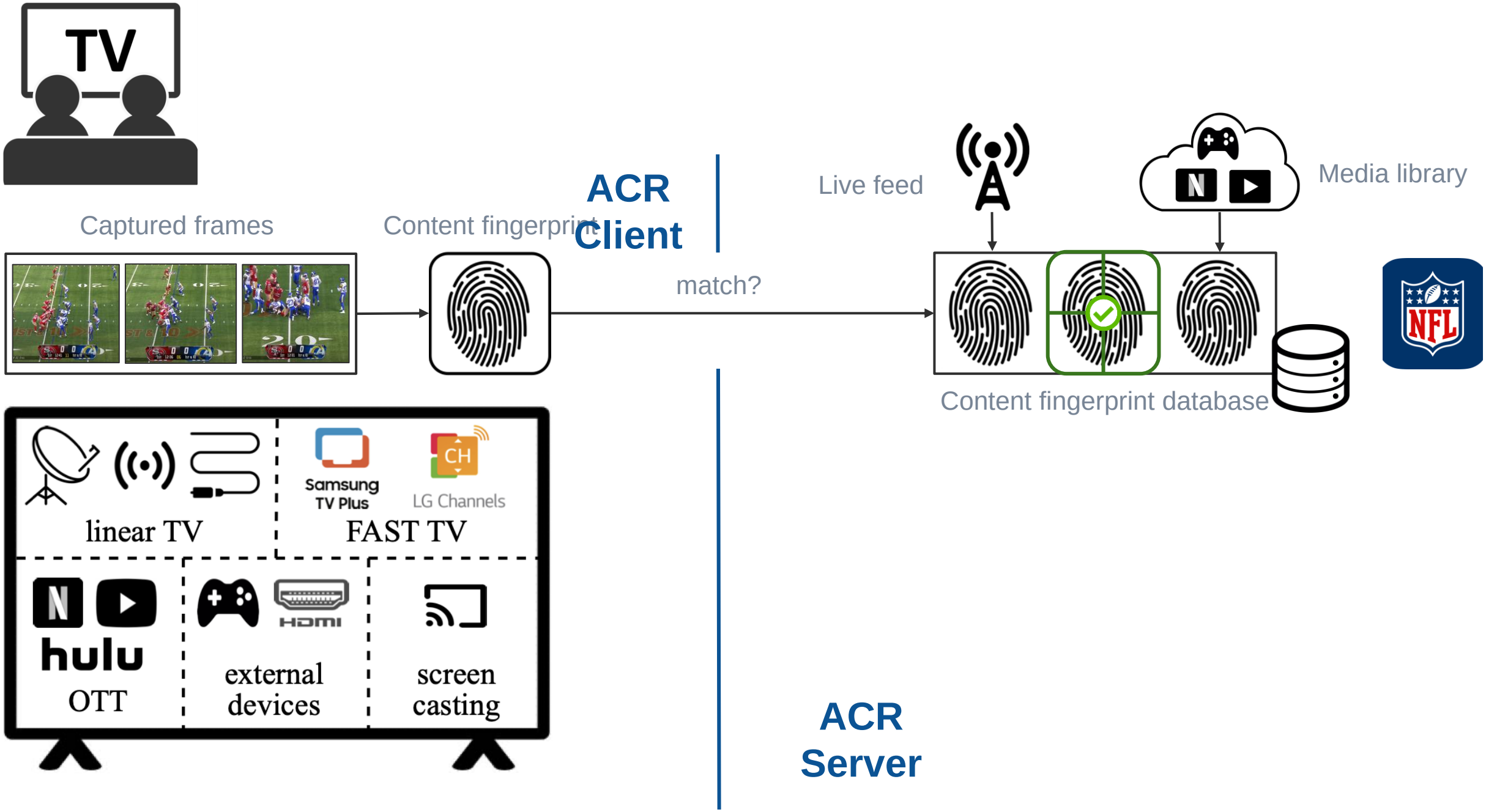
**ACR Client**

Content fingerprint database

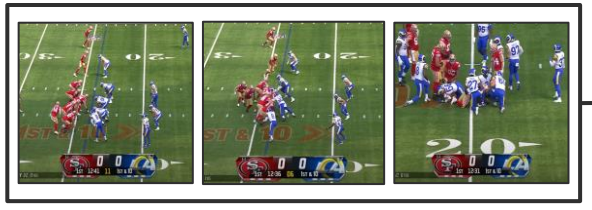



**ACR Server**


TV
Captured frames
Content fingerprint
ACR Client
Live feed
Media library
Content fingerprint database
linear TV
Samsung TV Plus
LG Channels
FAST TV
hulu
OTT
external devices
HDMI
screen casting
ACR Server


TV
Captured frames
Content fingerprint
ACR Client
match?
Live feed
Media library
Content fingerprint database
linear TV
Samsung TV Plus
LG Channels
FAST TV
hulu
OTT
external devices
screen casting
ACR Server


Captured frames



Content fingerprint

**ACR Client**

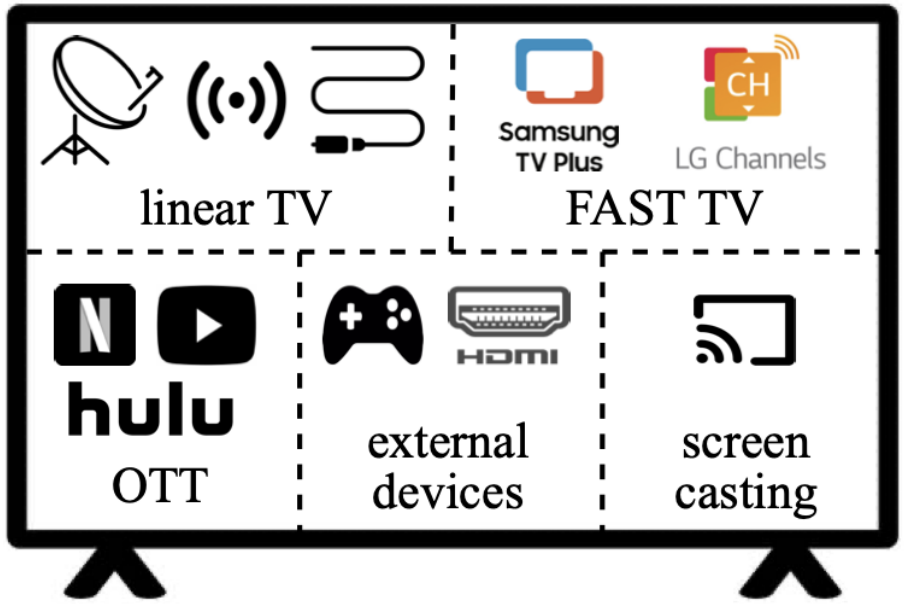
match?

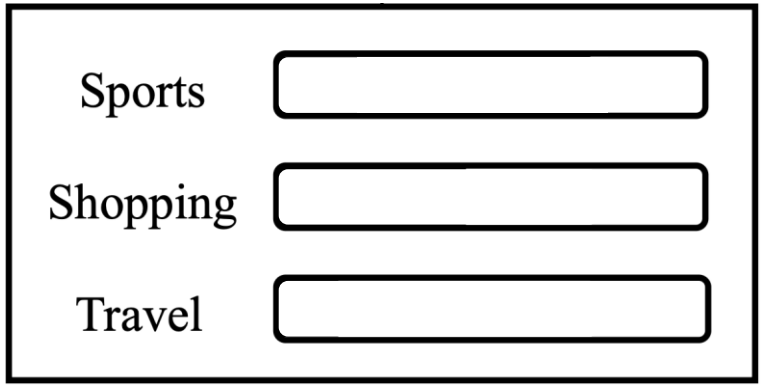
Live feed

Media library



Content fingerprint database

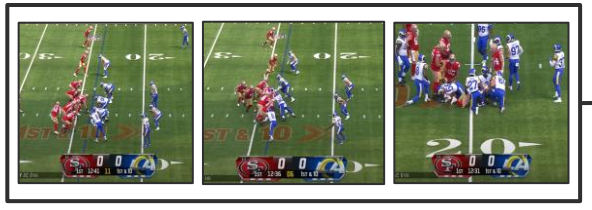



Audience segments

**ACR Server**


Captured frames



Content fingerprint

**ACR Client**

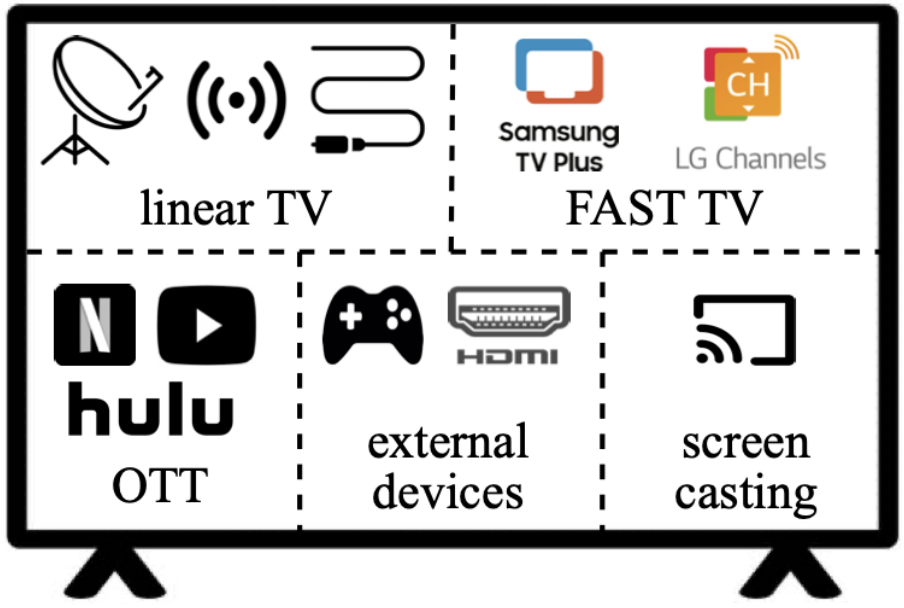
match?

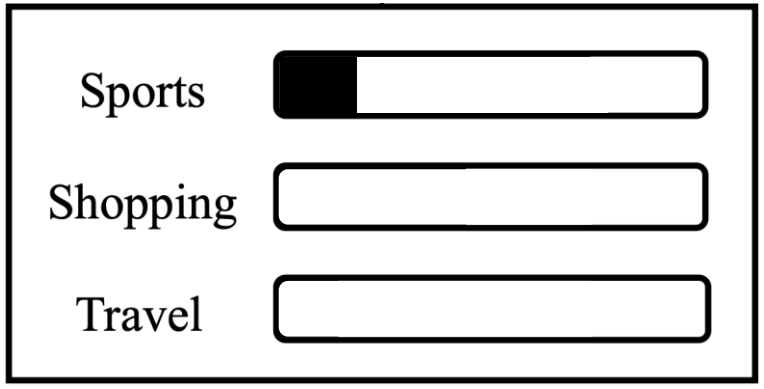
Live feed

Media library



Content fingerprint database




Audience segments

**ACR Server**

# How frequently does *ACR* capture snapshots of your viewing activities?

*It varies from manufacturer to manufacturer …*

*Captures video snapshots*

**500ms**

SAMSUNG

TIZEN™

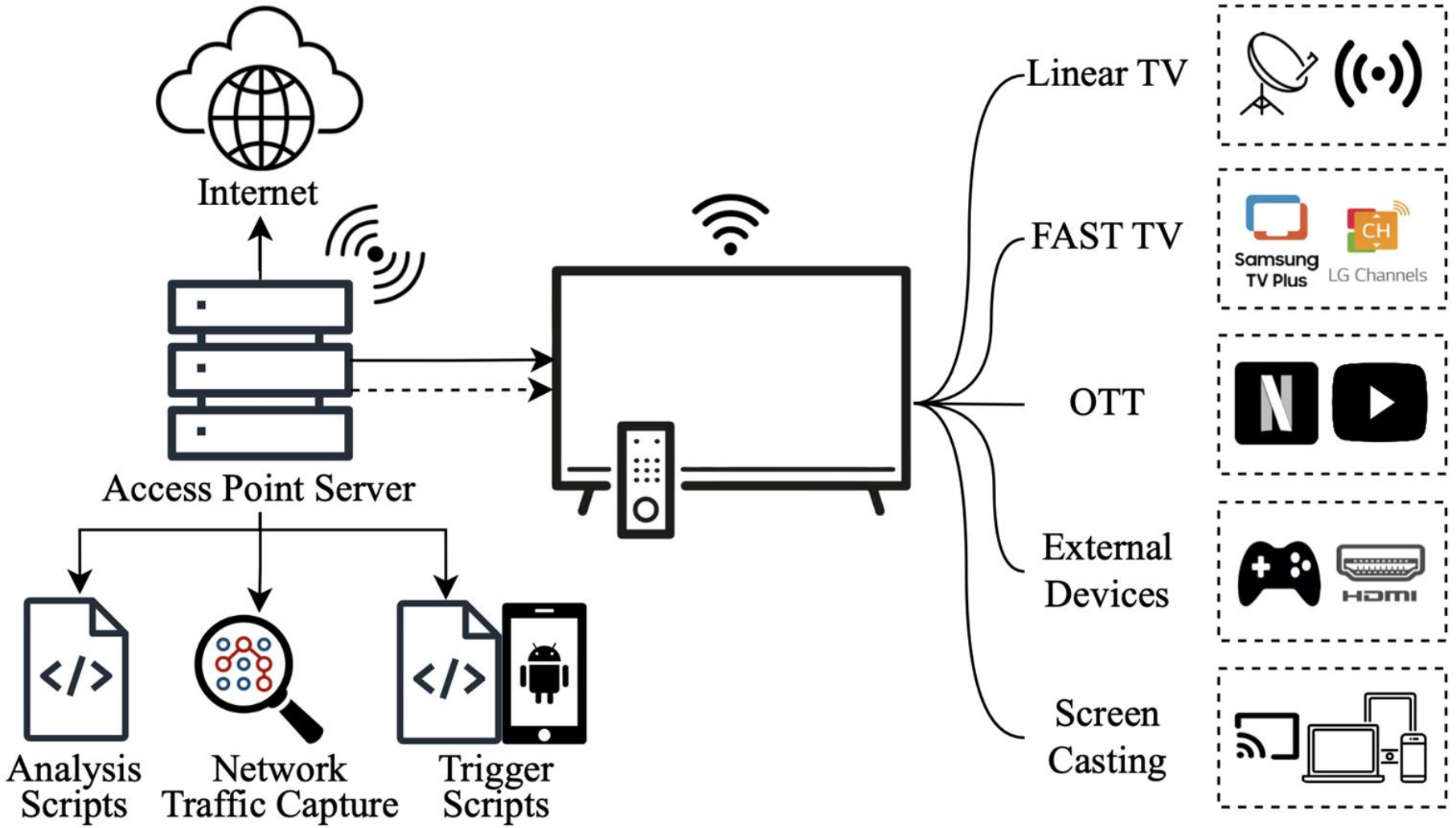
*Captures audio snapshots*

**10ms**

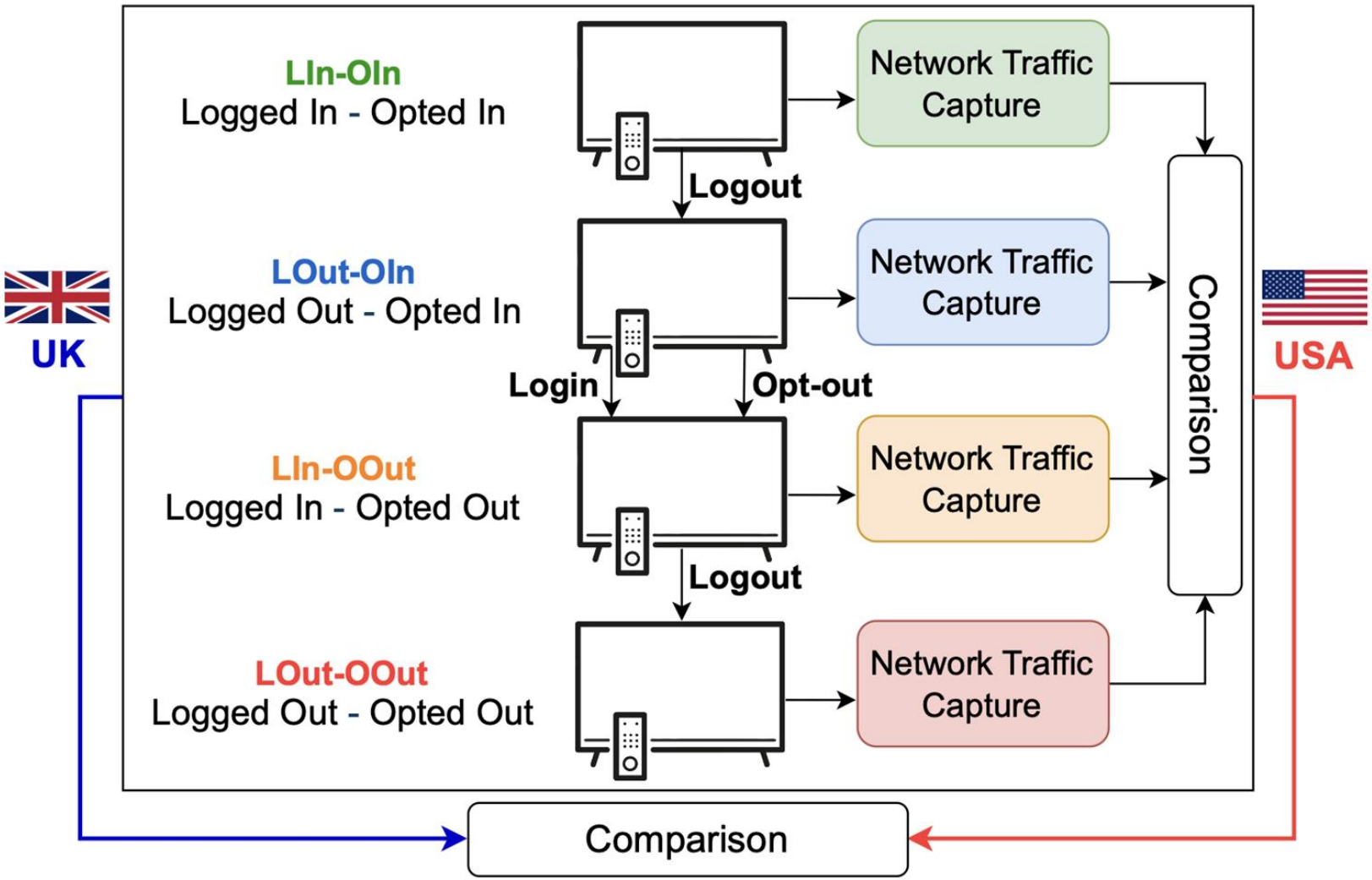
LG

webOS

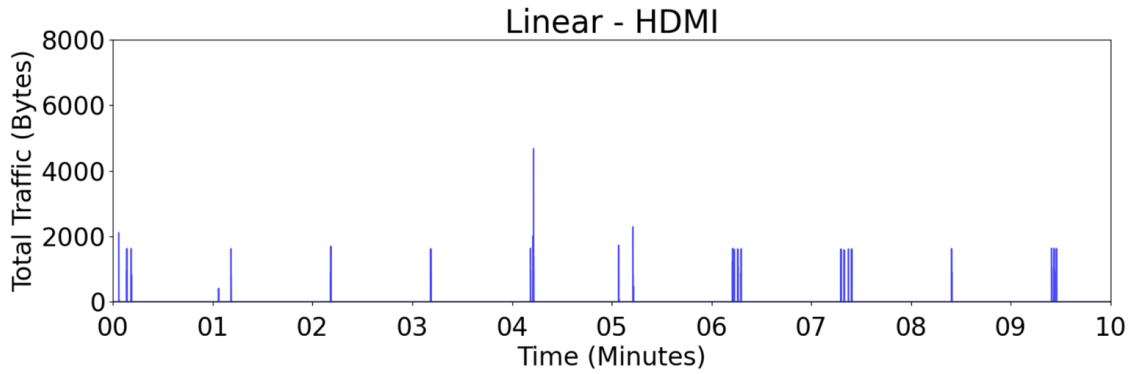
# Experimental Infrastructure

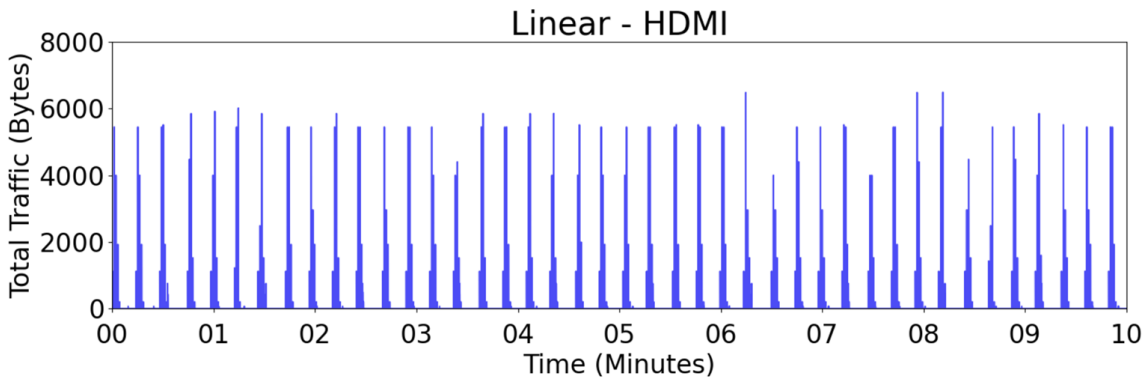


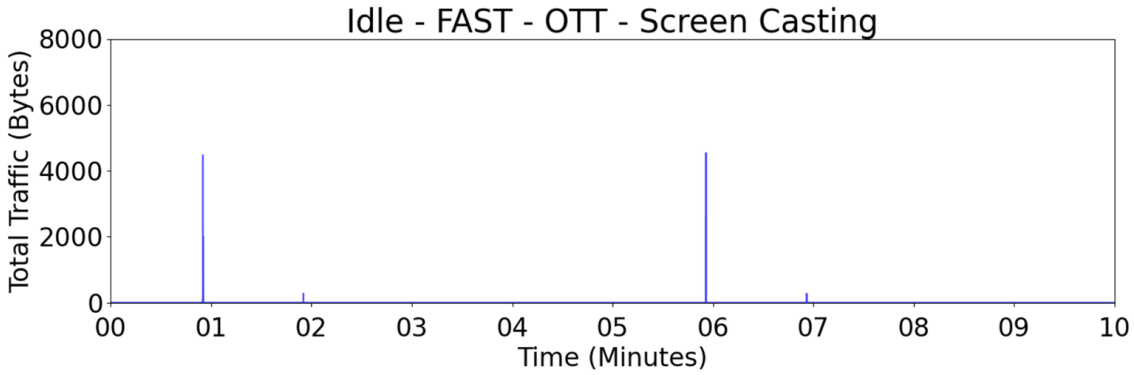
# Methodology

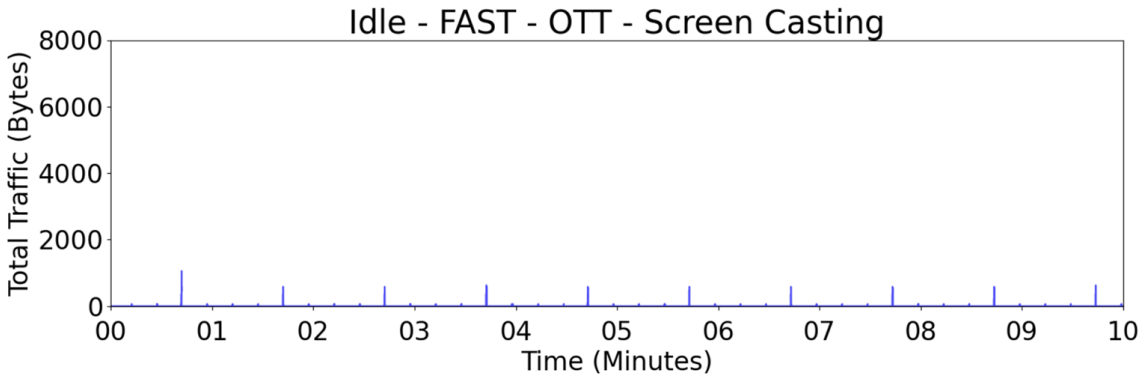


# Results: Comparison across Smart TV



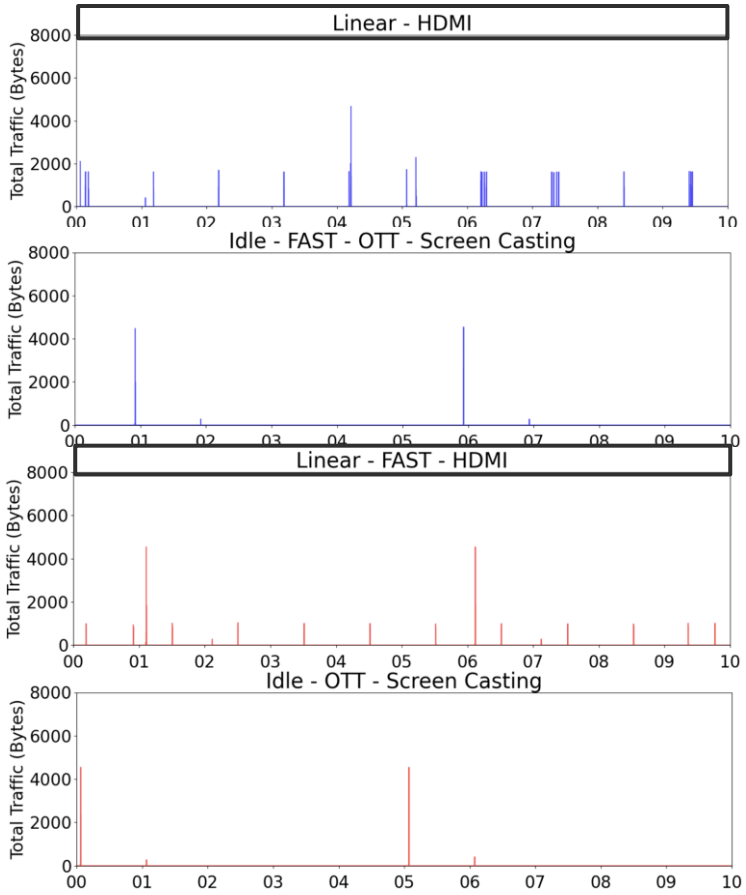



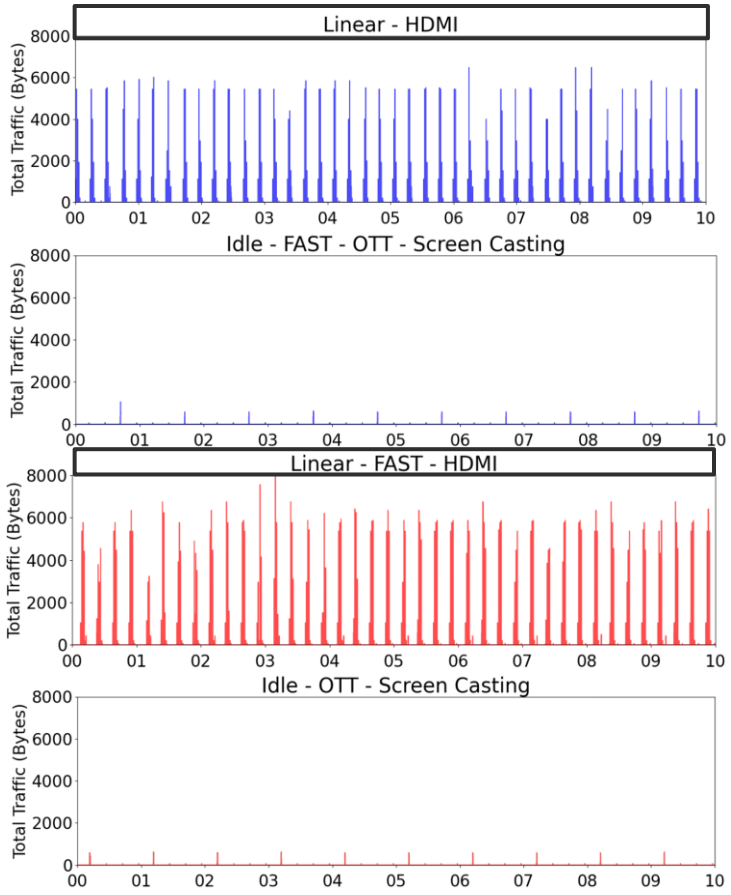

SAMSUNG

LG

# Smart TVs record your screen even *when used* as a “DUMB” display using HDMI

# Results: Comparison across the UK and US




SAMSUNG

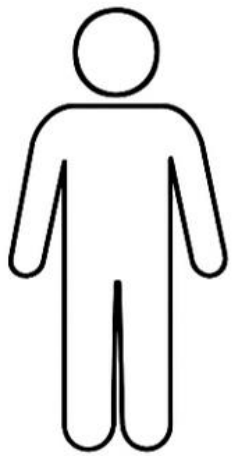
LG

01

# Reasons You Shouldn’t Use Smart Medical Devices

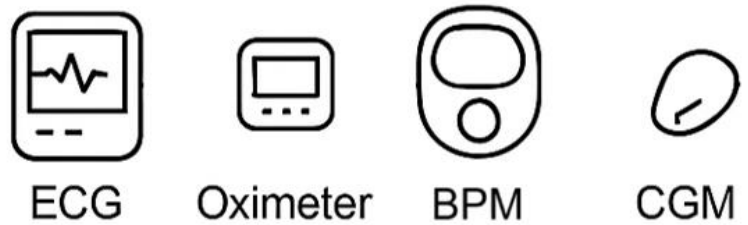
**Victim:**

- Blood pressure lability
- Heart arrhythmia
- Hypoxemia
- Diabetes

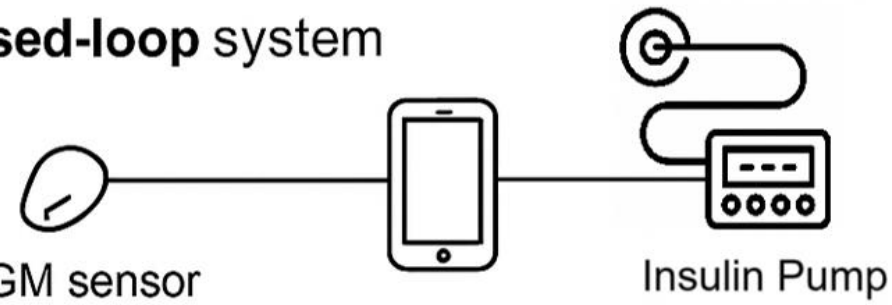


**System:**

**Open-loop** system

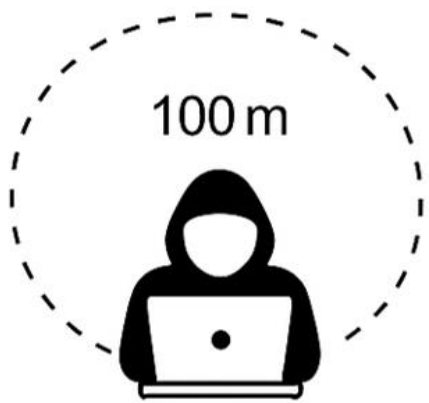



**Closed-loop** system



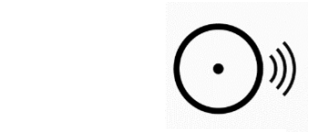

**Adversary:**

BLE 4.0 / BLE 5.0

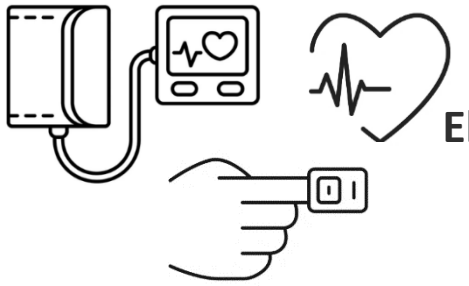



Passive (Sniffing/Eavesdropping) and
Active (MITM, DoS)

Dexcom ONE and
FreeStlye Libre2
**Continious Glocuse Monitors (CGM)**



**Wellue Blood Pressure Monitors (BPM)**



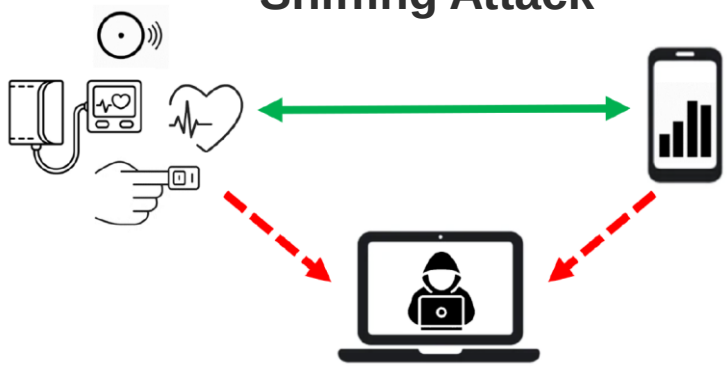
Oxylink and
SleepO2 1400
**Oximeters**

nRF52840 Nordic
Sniffer Dongle

SnapECG and
DuoEK Wellue
**Electrocardiograms (ECG)**

Bluetooth 4.0
Adapter USB
Dongles

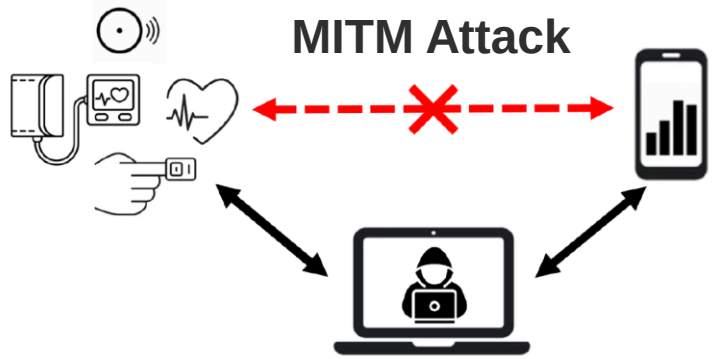
**Sniffing Attack**



iPhone 13
Pro/Google
Pixel 3

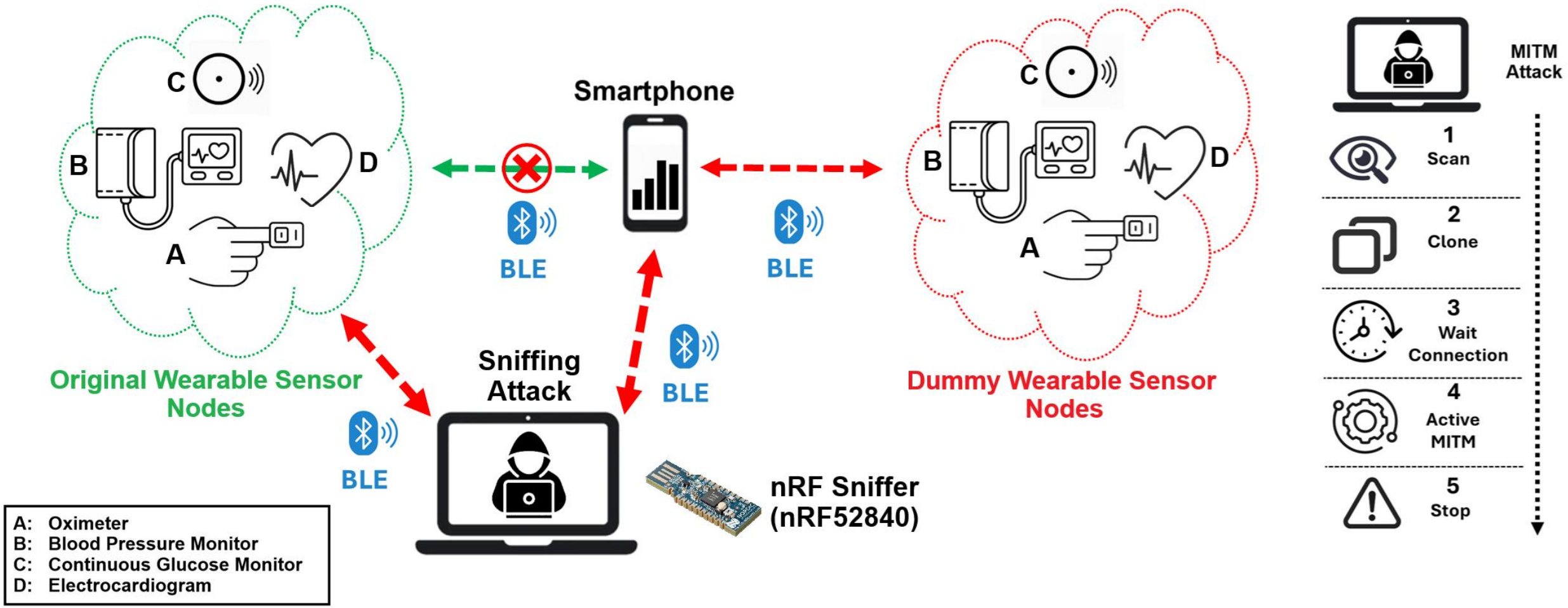
Wireshark Tool

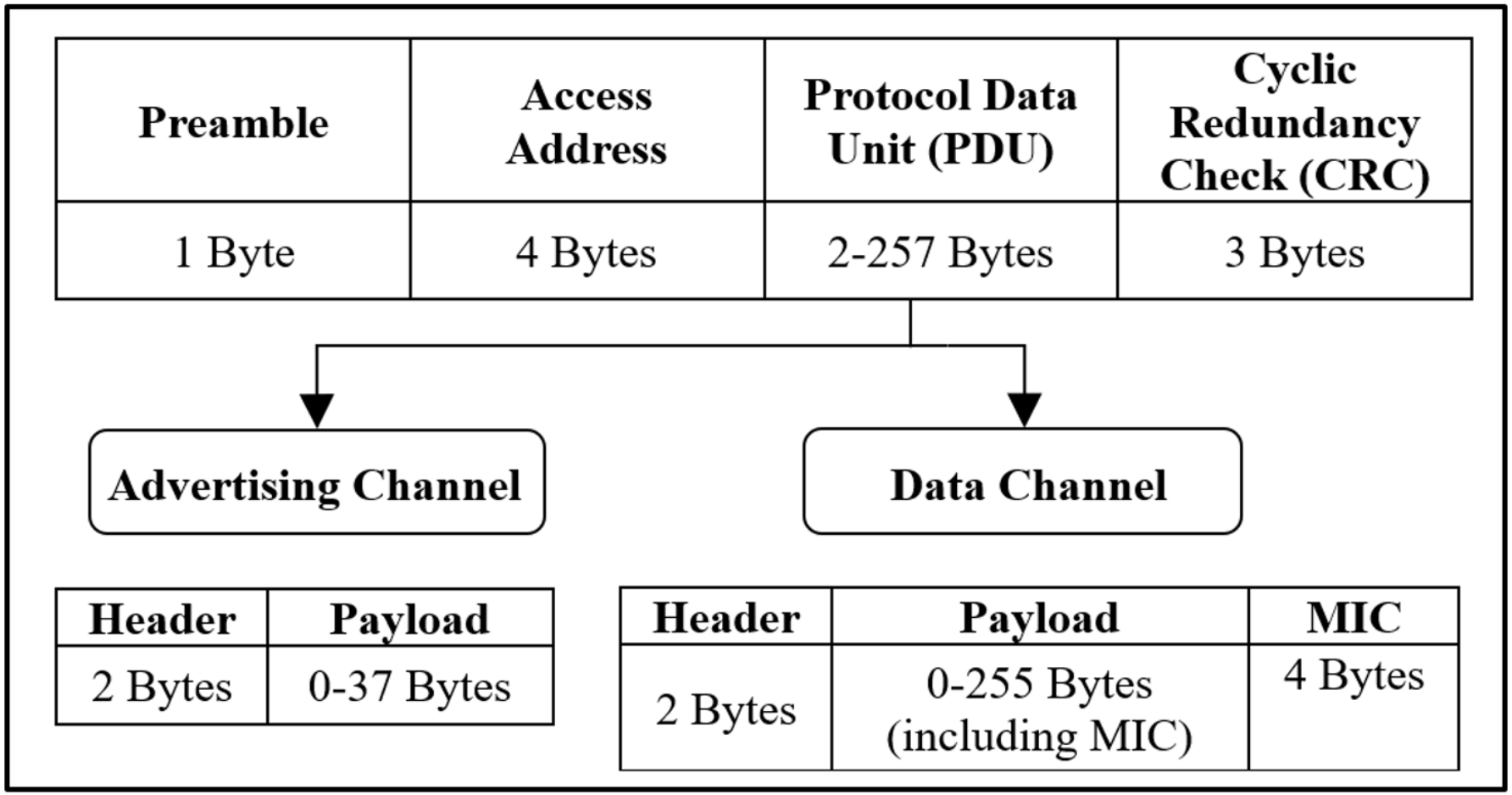
**MITM Attack**



iPhone 13
Pro/Google
Pixel 3

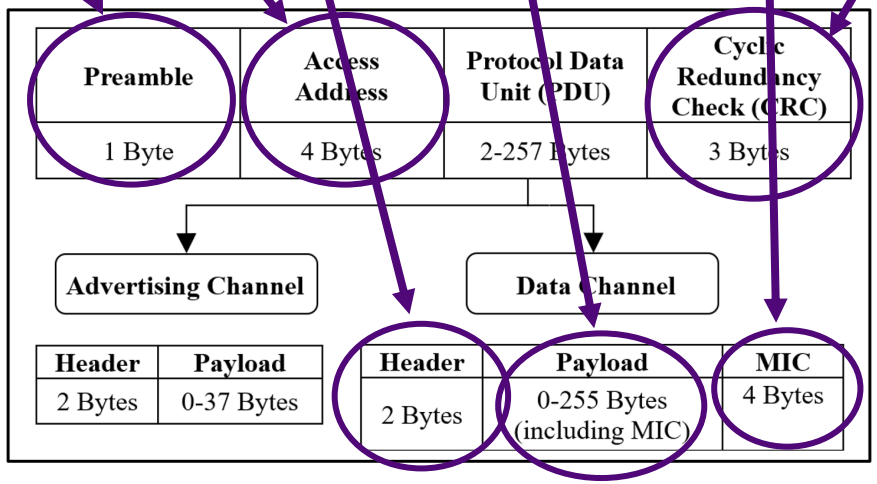
Kali Linux
Mirage Tool


C
B
D
A
Original Wearable Sensor Nodes
Smartphone
BLE
BLE
BLE
BLE
Sniffing Attack
nRF Sniffer (nRF52840)
C
B
D
A
Dummy Wearable Sensor Nodes
MITM Attack
1 Scan
2 Clone
3 Wait Connection
4 Active MITM
5 Stop
A: Oximeter
B: Blood Pressure Monitor
C: Continuous Glucose Monitor
D: Electrocardiogram


Preamble
Access Address
Protocol Data Unit (PDU)
Cyclic Redundancy Check (CRC)
1 Byte
4 Bytes
2-257 Bytes
3 Bytes
Advertising Channel
Data Channel
Header
Payload
2 Bytes
0-37 Bytes
Header
Payload
MIC
2 Bytes
0-255 Bytes (including MIC)
4 Bytes

**Oxylink Oximeter Encrypted Payload Content**:

Handle “0x19”: 5500ff00000d00615e00000000004200070e0100




615e00000000

61 (hex) = 97 (dec)

97% Oxygen Level

5e (hex) = 94 (dec)

94/min Heart Rate

**???**

**Original:** Handle “0x19”: 5500ff00000d00615e00000000004200070e0100

**Key:** “39”

**Replay:** Handle “0x19”: 5500ff00000d00604100000000005500000501 00

**Key:** “db”

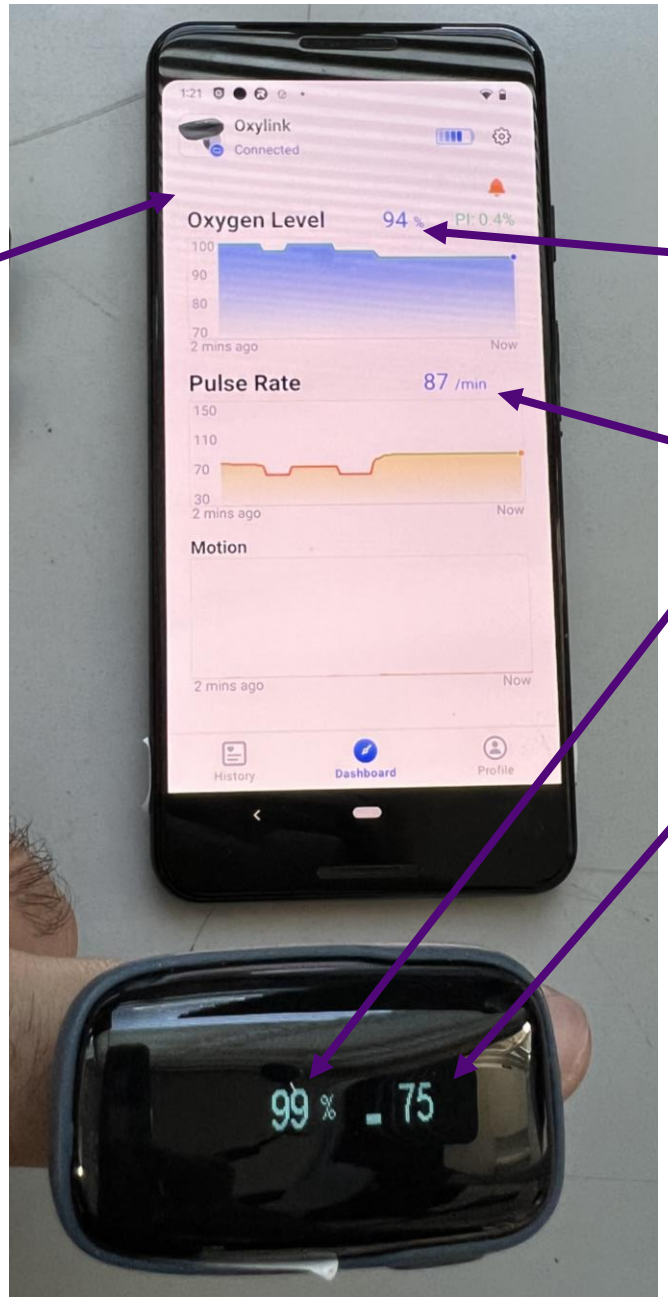
60 (hex) = 96 (dec)

96% Oxygen Level

41 (hex) = 65 (dec)

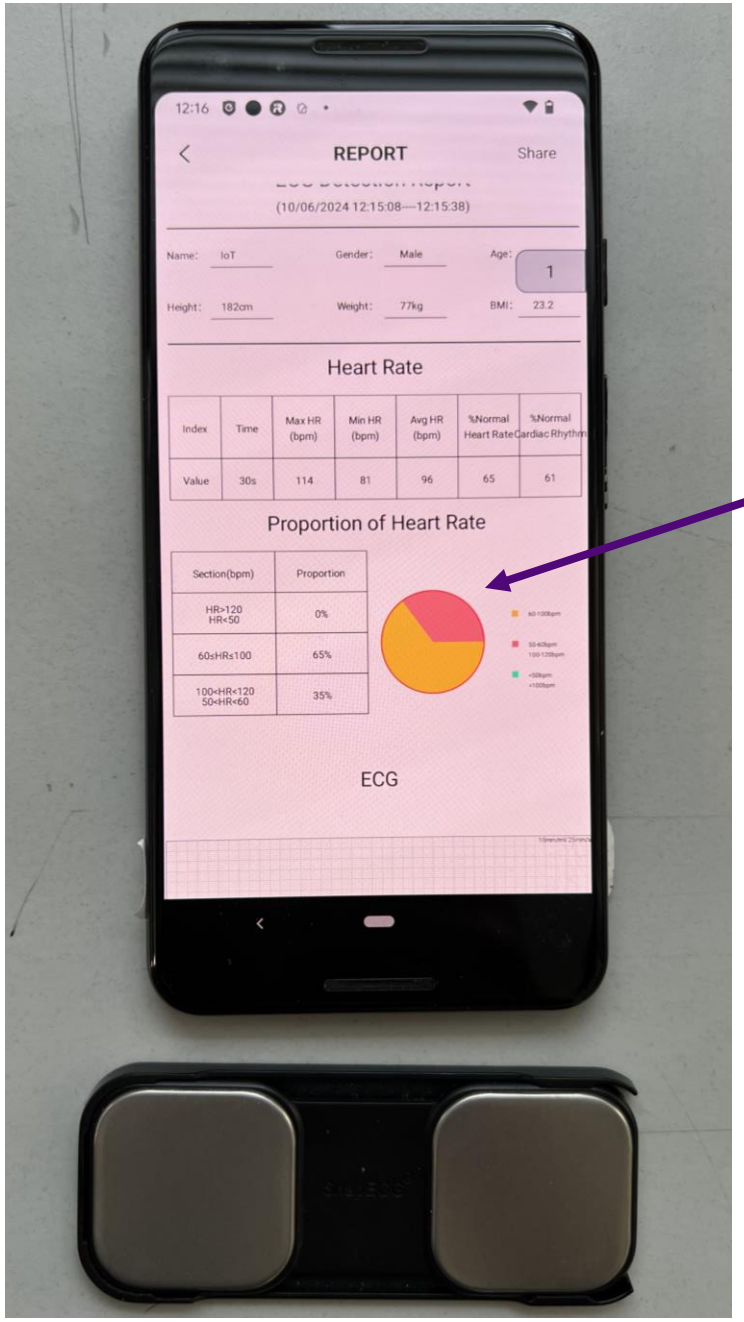
65/min Heart Rate

ViHealth App
Real-time Data
Manipulation

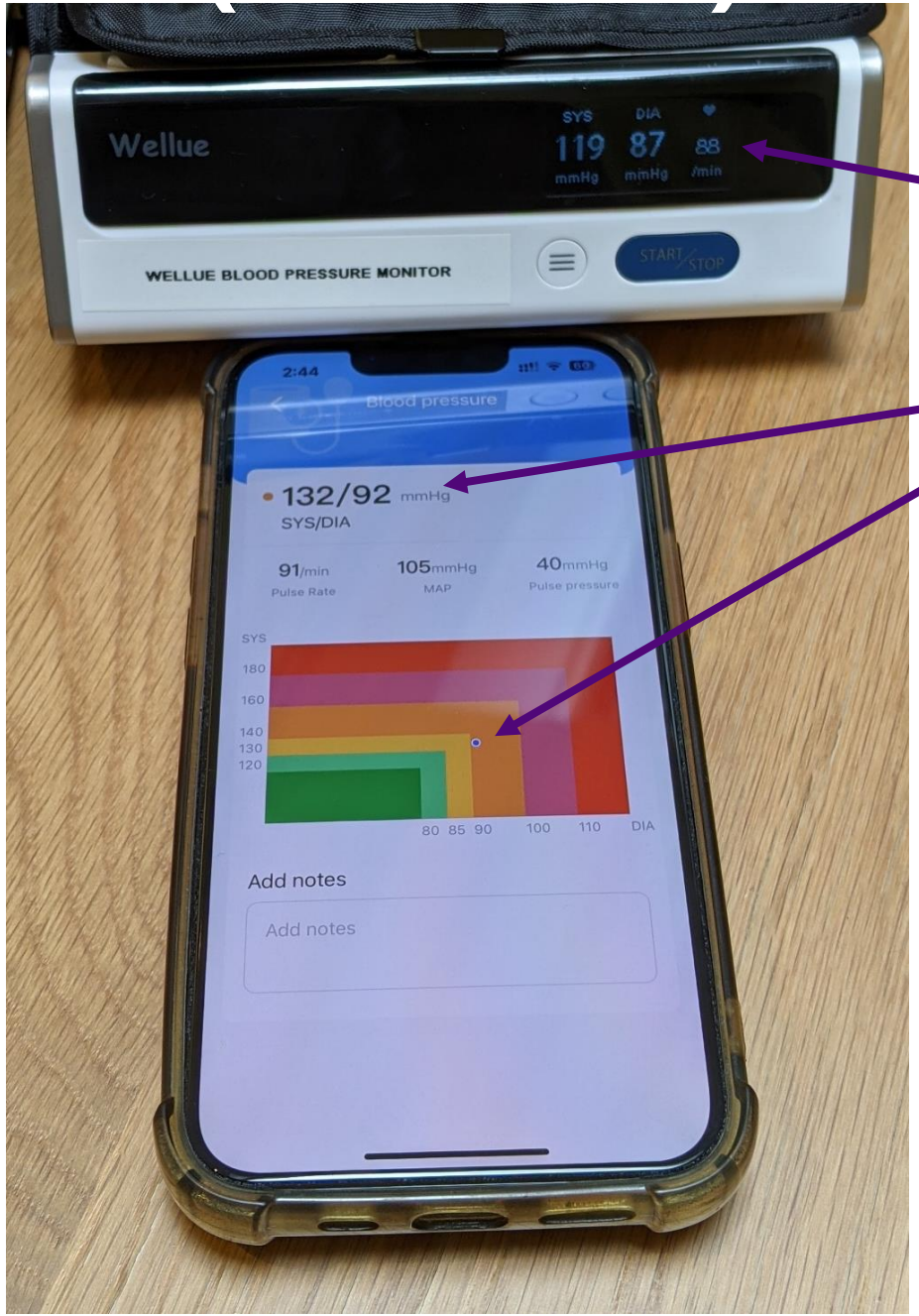



Oxygen Level
Manipulation

Pulse Rate
Manipulation




Unhealthy Report




Typical Normal Reading

Hypertension Stage 1

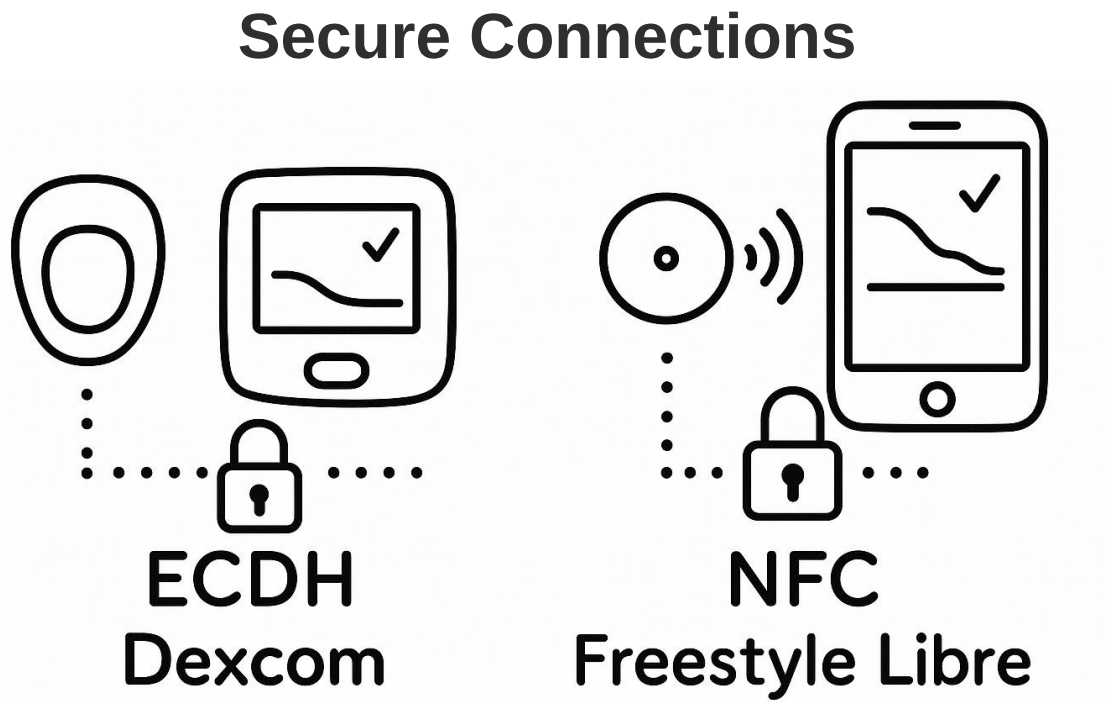
Secure Connections (for initial pairing and keys exchange):

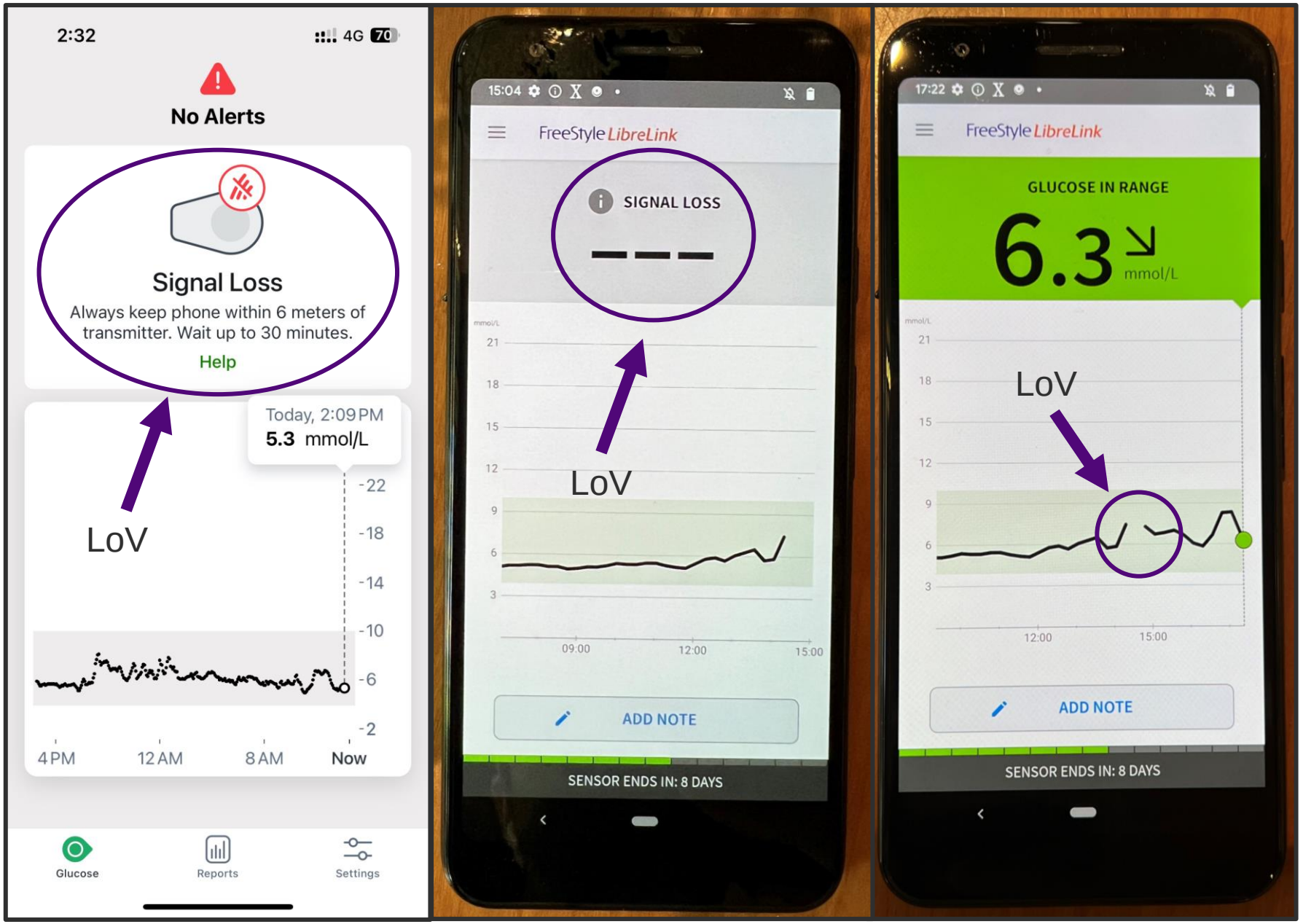
- **Elliptic Curve Diffie-Hellman (ECDH)**.

  → Private keys → Public keys → ECDH → Shared secret →
  KDFs → rand → EDIV → IVs →


Session key

- **Near Field Communication (NFC)**.

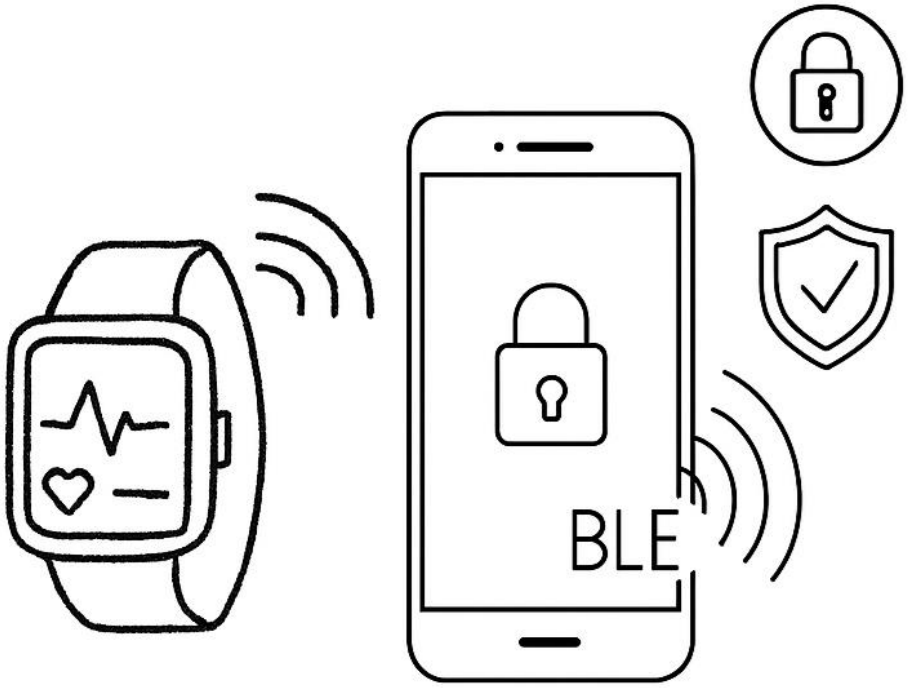



2:32
4G
No Alerts
Signal Loss
Always keep phone within 6 meters of transmitter. Wait up to 30 minutes.
Help
Today, 2:09 PM
5.3 mmol/L
LoV
22
18
14
10
6
2
4 PM
12 AM
8 AM
Now
Glucose
Reports
Settings
15:04
FreeStyle LibreLink
SIGNAL LOSS
LoV
21
18
15
12
9
6
3
09:00
12:00
15:00
ADD NOTE
SENSOR ENDS IN: 8 DAYS
17:22
FreeStyle LibreLink
GLUCOSE IN RANGE
6.3
mmol/L
LoV
21
18
15
12
9
6
3
12:00
15:00
ADD NOTE
SENSOR ENDS IN: 8 DAYS

| Devices | Types of Attacks | | | |
|---|---|---|---|---|
| | Sniffing (Eavesdropping) | Passive MITM (Eavesdropping) | Active MITM (Data Manipulation) | DoS (Loss of View) |
| SnapECG **(ECG)** | ✓ | ✓ | ✓ | ✓ |
| DuoEK Wellue **(ECG)** | ✓ | ✗ | ✗ | ✓ |
| OXYLINK **(Oximeter)** | ✓ | ✓ | ✓ | ✓ |
| SleepO2 1400 **(Oximeter)** | ✓ | ✓ | ✓ | ✓ |
| Wellue BP2A 2031 **(BPM)** | ✓ | ✓ | ✓ | ✓ |
| Dexcom ONE **(CGM)** | ✓ | ✗ | ✗ | ✓ |
| FreeStyle Libre 2 **(CGM)** | ✓ | ✗ | ✗ | ✓ |

- Significant **vulnerabilities** in BLE-enabled Wearable Sensor Nodes.

- Recommendations for **improving security**:
  - Stronger encryption
  - Multi-layered approach
  - Secure authentication
  - Real-time monitoring of device performance and security status.
- Call to action for **manufacturers & stakeholders** to address these issues.



# Agenda

01 **Problem: IoT Devices Expose Information Over the Internet**

Reasons you shouldn’t watch TV
Reasons you shouldn’t use smart medical devices.

02 **Privacy and Security Certification/Regulation**

EU Cyber Resilience Act (CRA)
GDPR

03 **IoT Automating Testing and Compliance**

IoTrim ++
Black box assessment

04 **Standards**

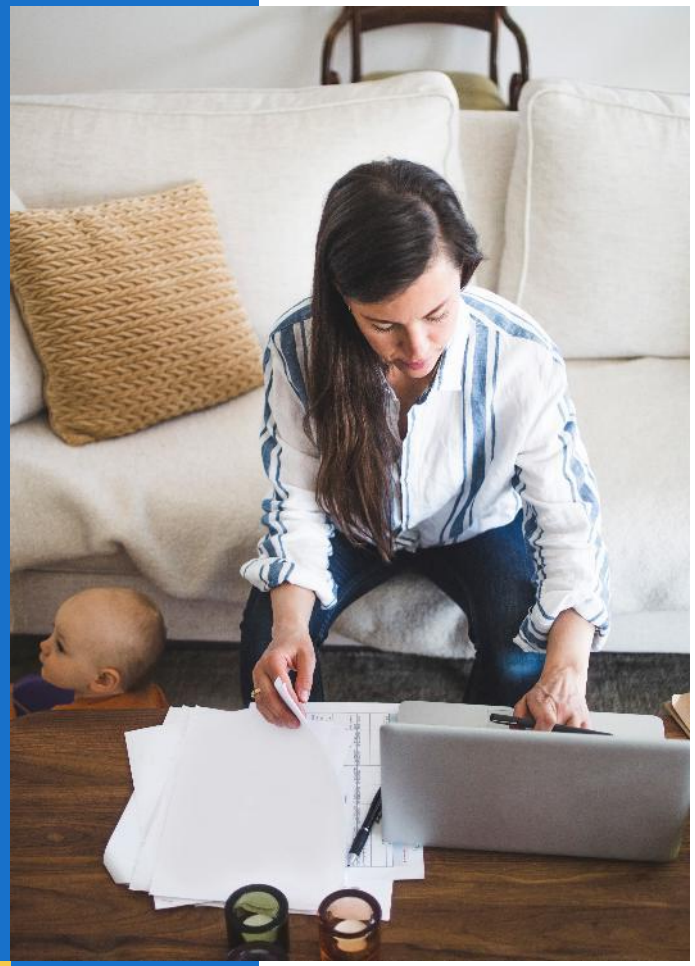
Standardization request
ETSI/CEN-CENELC WGs

05 **Gaps**

IoT Manufactures
SMEs

06 **Conclusion**

What’s next?



02

# Big Mess?

# EU Cyber Resilience Act (CRA)

- In the general case, they will do a self-assesment
- If their product is on the list of “important” products, they will either need to follow standards or do a third-party assessment
- If their product is on the critical list, they will need to undergo a third-party assessment and possibly be certified in the future.
- FOSS (Free and Open Source Software) products do self assessments except for critical products

# GDPR

- Information Commissioner's Office (ICO) IoT guidelines [to be released in June for consultation]
- IoT device manufacturers must ensure data protection by design and by default
- They are obligated to provide clear, accessible information to users about data collection

# Agenda

01 **Problem: IoT Devices Expose Information Over the Internet**

Reasons you shouldn’t watch TV
Reasons you shouldn’t use smart medical devices.

02 **Privacy and Security Certification/Regulation**

EU Cyber Resilience Act (CRA)
GDPR

03 **IoT Automating Testing and Compliance**

IoTrim ++
Black box assessment

04 **Standards**

Standardization request
ETSI/CEN-CENELC WGs

05 **Gaps**

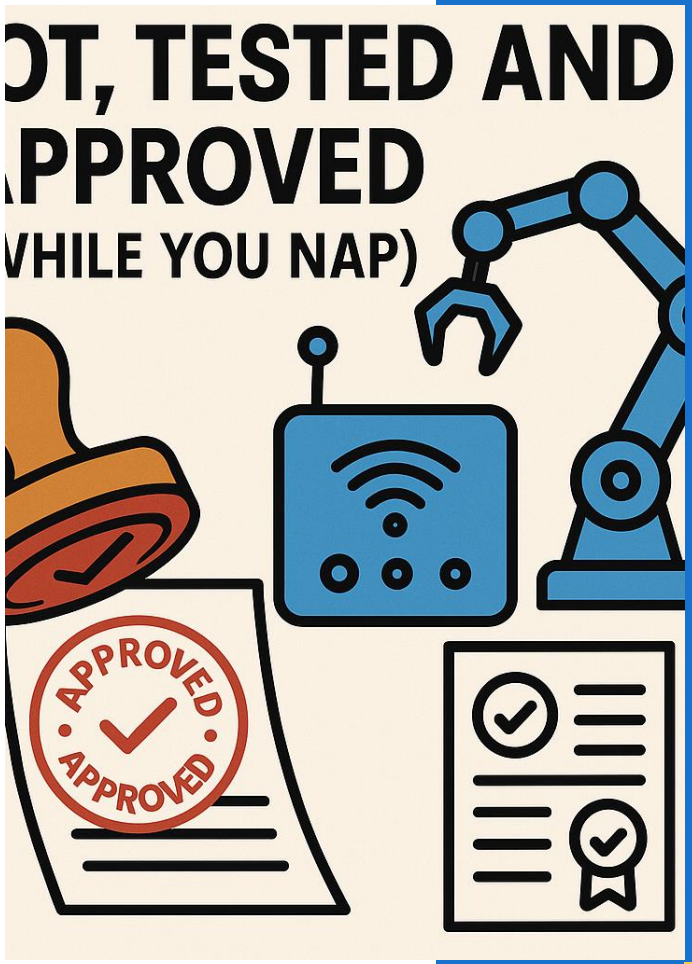
IoT Manufactures
SMEs

06 **Conclusion**

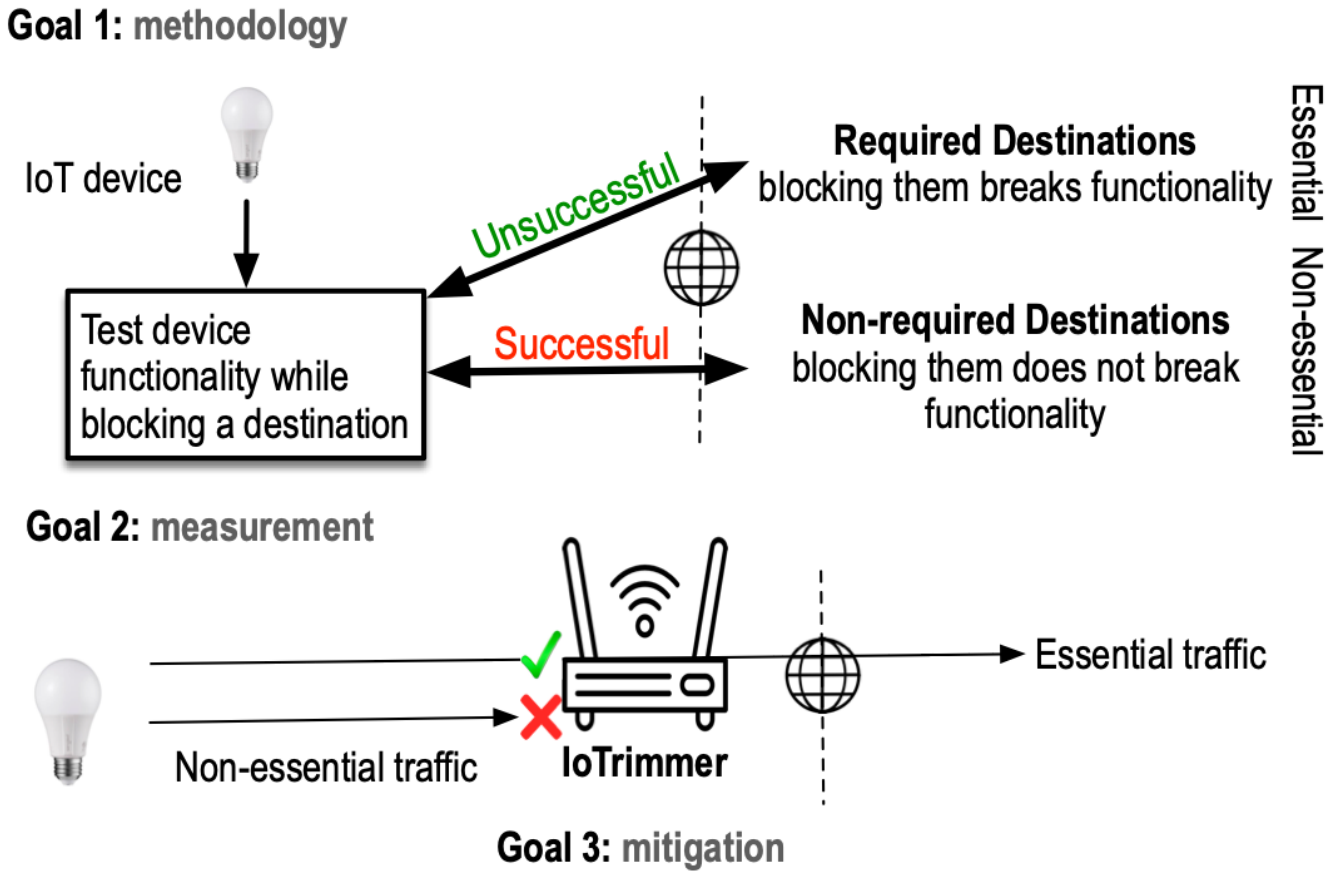
What’s next?

03

# Compliance Without Tears: Let the IoT Do It



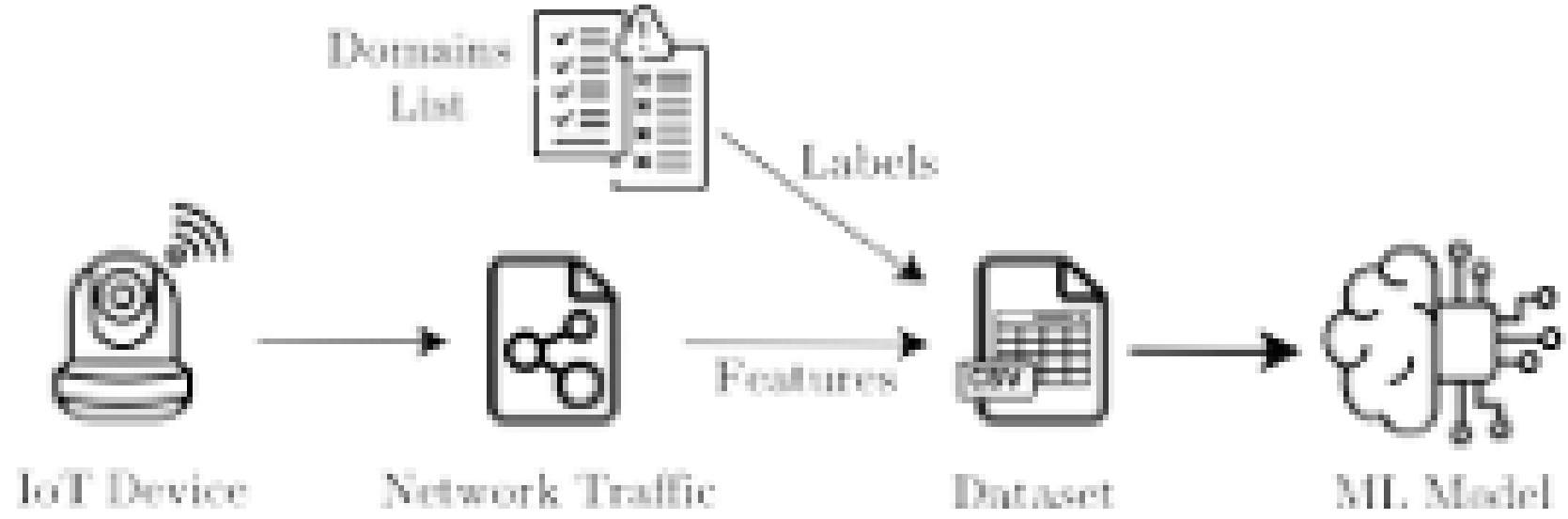
# IoTrim++



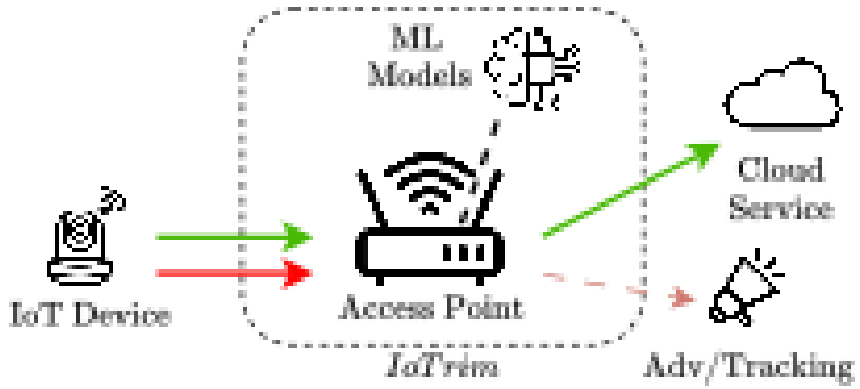

/ Generalizable

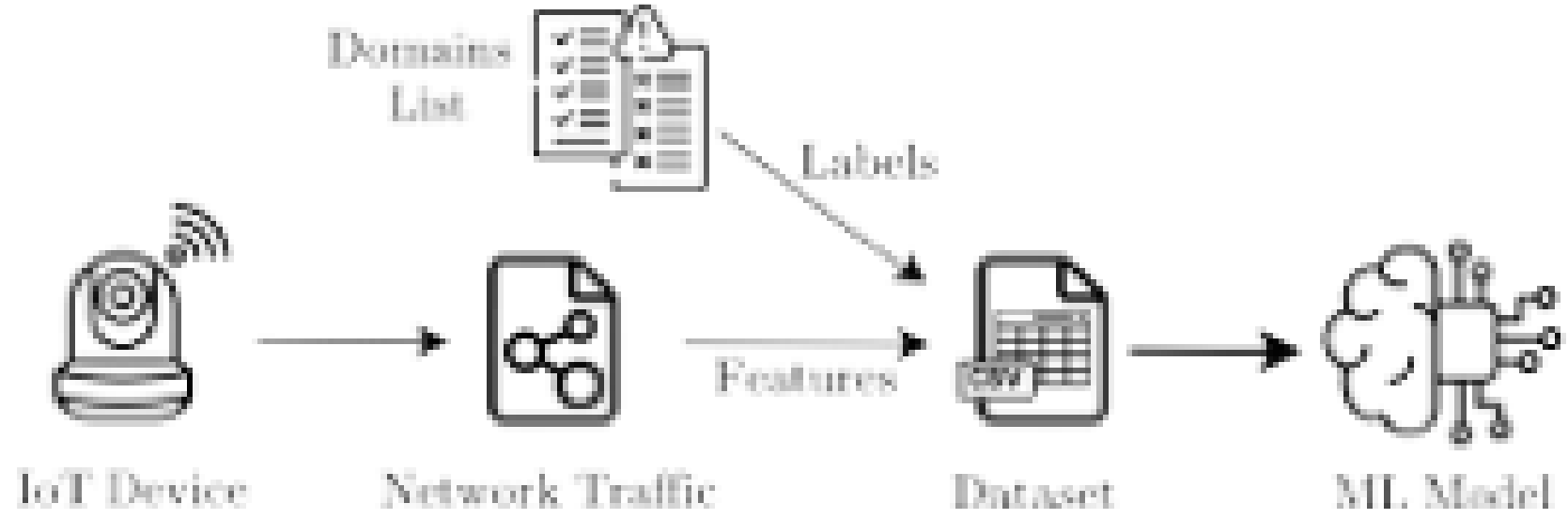
/ Self adaptive

/ Accurate IoT blocker

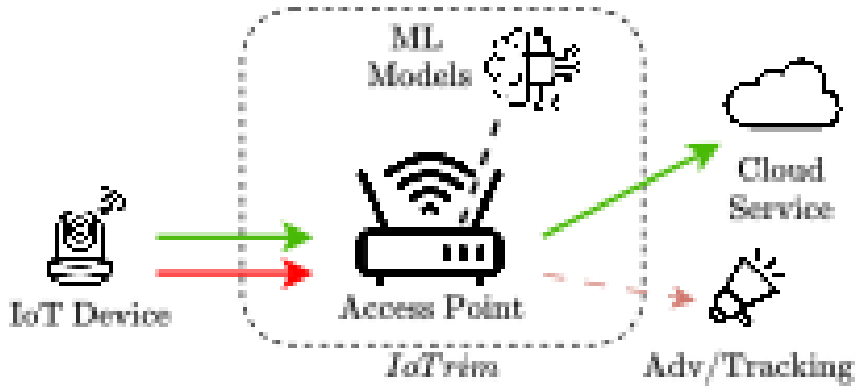



# Automatically detecting non-essential destinations

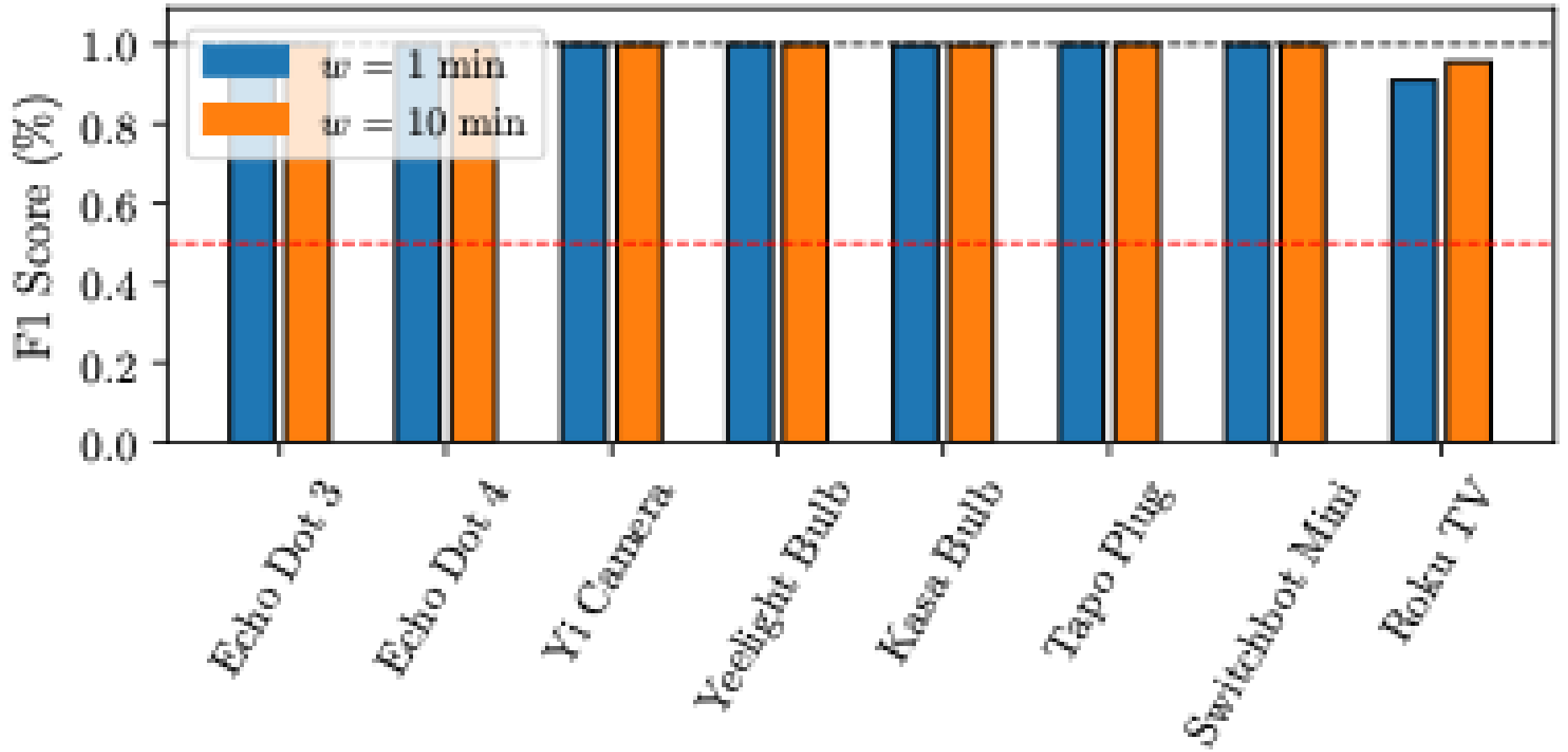





# Automatically detecting non-essential destinations

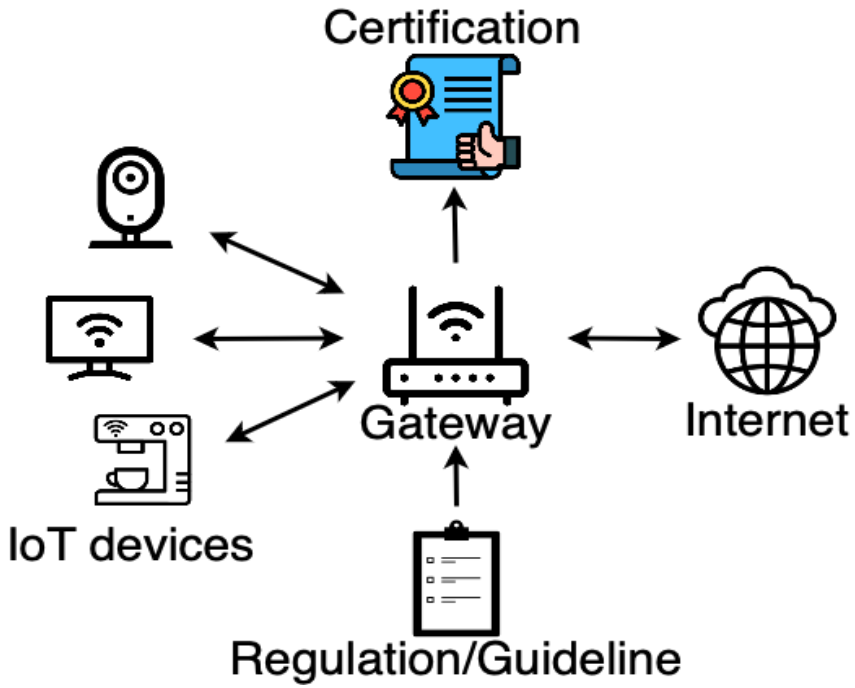


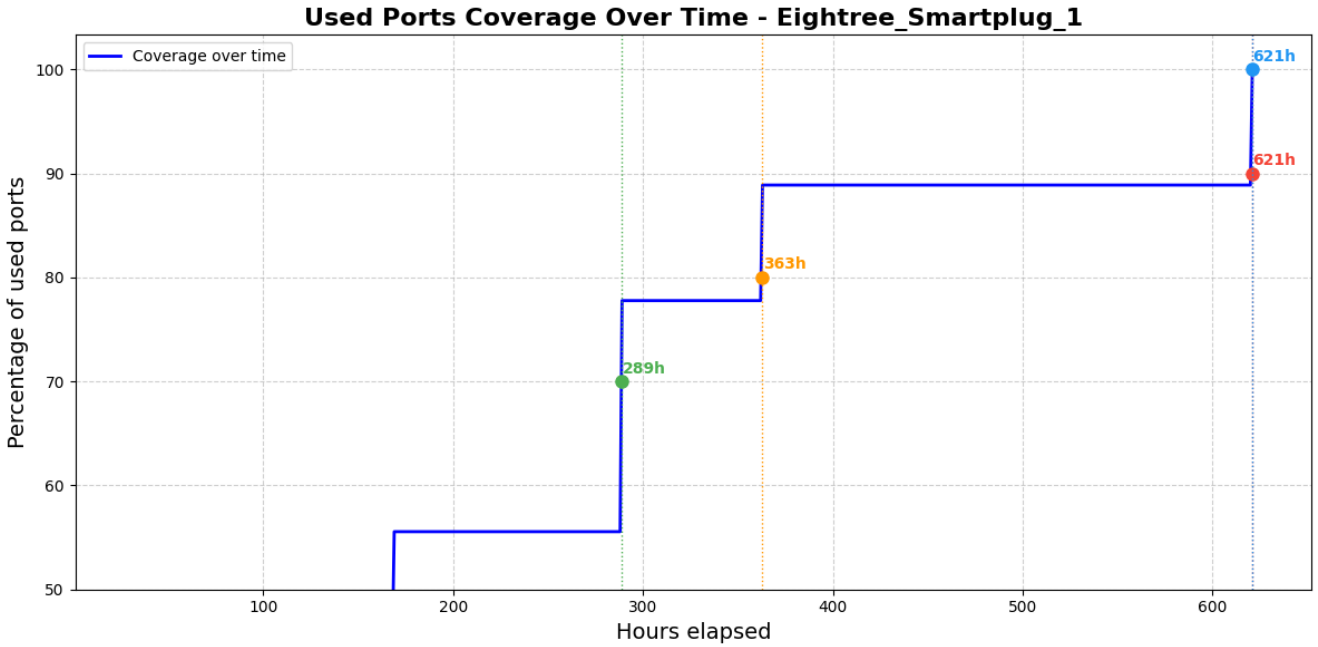
# Automatically detecting non-essential destinations



# Black Box Assessment

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




# Testing Requirements

For how long do we need to test the device?

Used Ports

# Agenda

01 **Problem: IoT Devices Expose Information Over the Internet**

Reasons you shouldn't watch TV
Reasons you shouldn't use smart medical devices.

02 **Privacy and Security Certification/Regulation**

EU Cyber Resilience Act (CRA)
GDPR

03 **IoT Automating Testing and Compliance**

IoTrim ++
Black box assessment

04 **Standards**

Standardization request
ETSI/CEN-CENELC WGs

05 **Gaps**

IoT Manufactures
SMEs

06 **Conclusion**

What's next?

04

# When in Doubt, Create Another Standard!

# CRA Standardization Effort

## Current Focus Areas

- Mapping existing standards to CRA requirements
- Defining **secure lifecycle processes** for digital products
- Ensuring **interoperability** and **compliance frameworks**
- Supporting **conformity assessment** procedures

## Impact

- Streamlined compliance for EU manufacturers
- Stronger cybersecurity baseline across digital products
- Cross-sector adoption of harmonized security standards

## ETSI

- Leading development of technical standards and specifications for ICT
- Key standards: ETSI EN 303 645 (IoT security baseline)

## CEN-CENELEC

- Aligning and integrating standards into the EU regulatory framework
- Developing Harmonized Standards (HAS) for CRA compliance
  Coordinating with EC and stakeholders through JTC 13 (Cybersecurity & Data Protection)

# Agenda

01 **Problem: IoT Devices Expose Information Over the Internet**

Reasons you shouldn’t watch TV
Reasons you shouldn’t use smart medical devices.

02 **Privacy and Security Certification/Regulation**

EU Cyber Resilience Act (CRA)
GDPR

03 **IoT Automating Testing and Compliance**

IoTrim ++
Black box assessment

04 **Standards**

Standardization request
ETSI/CEN-CENELC WGs

05 **Gaps**

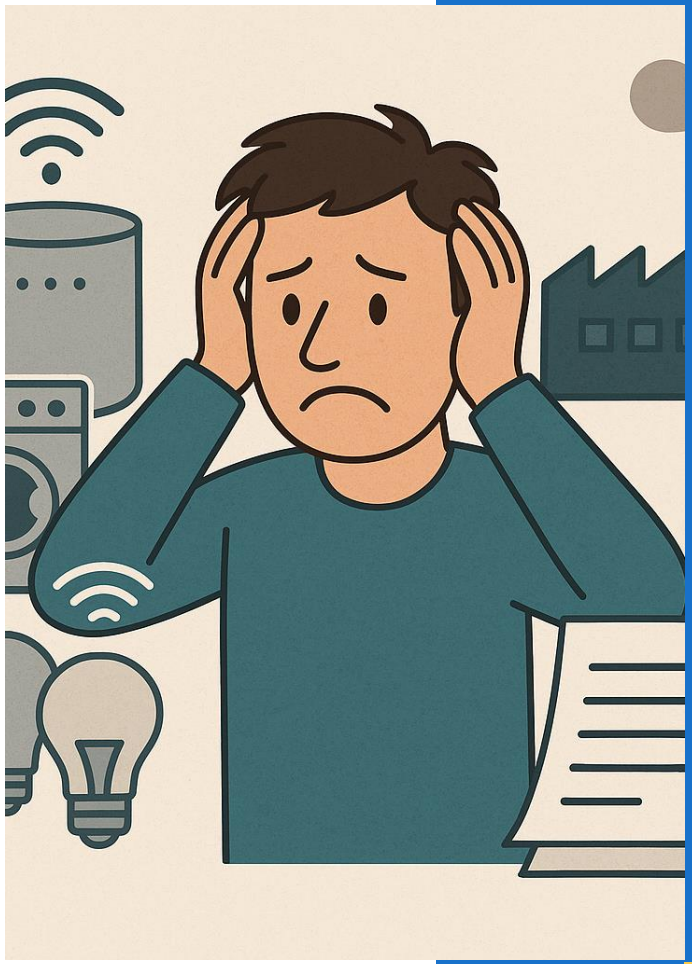
IoT Manufactures
SMEs

06 **Conclusion**

What’s next?

05

# When Your Toaster Is Smarter Than Your Compliance Process



# Gap

IoT Manufactures and SMEs need help!

# Gap

How can we create a standard based on network behaviour of IoT devices?

# Helping Manufacturers and SMEs to be Automatically Compliant

## Mulini

One click. More security and privacy.

## RIPE NCC Community Projects Fund

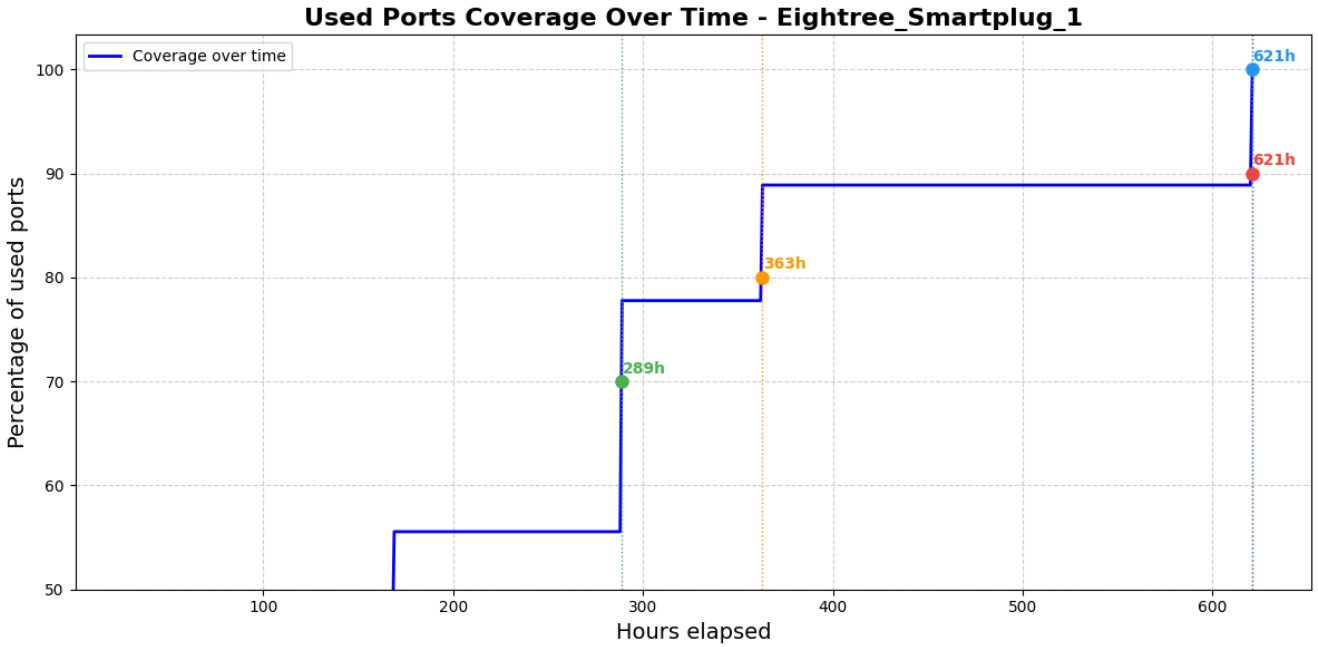
The project automates IoT security checks using machine learning and real-world monitoring to ensure compliance with cybersecurity standards.

## Final Goal

Open tool for developers and regulatory compliance auditors for independent compliance checking and security threat detection.

## Stakeholders involvement

SMEs
IoT Manufacturers
Policy Makers




# Testing Requirements

For how long do we need to test the device?

Used Ports

# Help!

If interested, please get in touch!

Internet of Things Working Group

# Agenda

01 **Problem: IoT Devices Expose Information Over the Internet**

Reasons you shouldn’t watch TV
Reasons you shouldn’t use smart medical devices.

02 **Privacy and Security Certification/Regulation**

EU Cyber Resilience Act (CRA)
GDPR

03 **IoT Automating Testing and Compliance**

IoTrim ++
Black box assessment

04 **Standards**

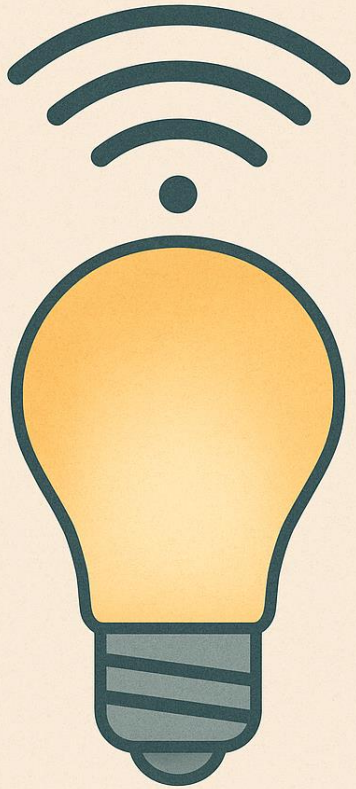
Standardization request
ETSI/CEN-CENELC WGs

05 **Gaps**

IoT Manufactures
SMEs

06 **Conclusion**

What’s next?



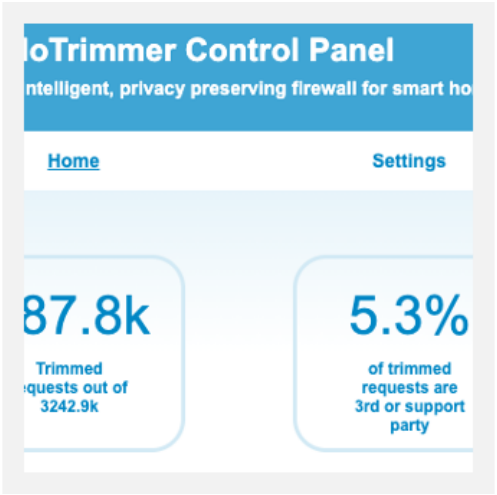
06

# Making Compliance So Easy, Even Your Lightbulb Could Do It

# What's Next?

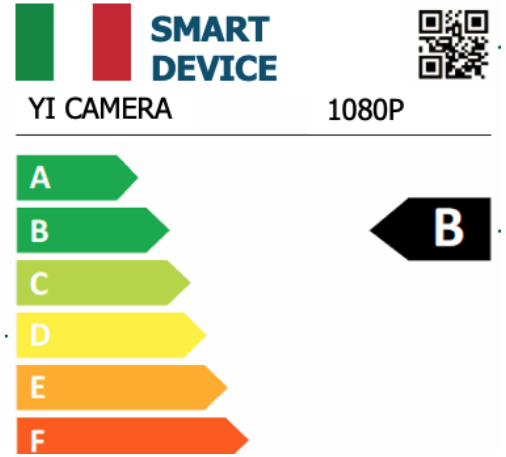
**Privacy Preserving IoT Security Management**

- Real IoT gateway




**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

# Thank You

mulini