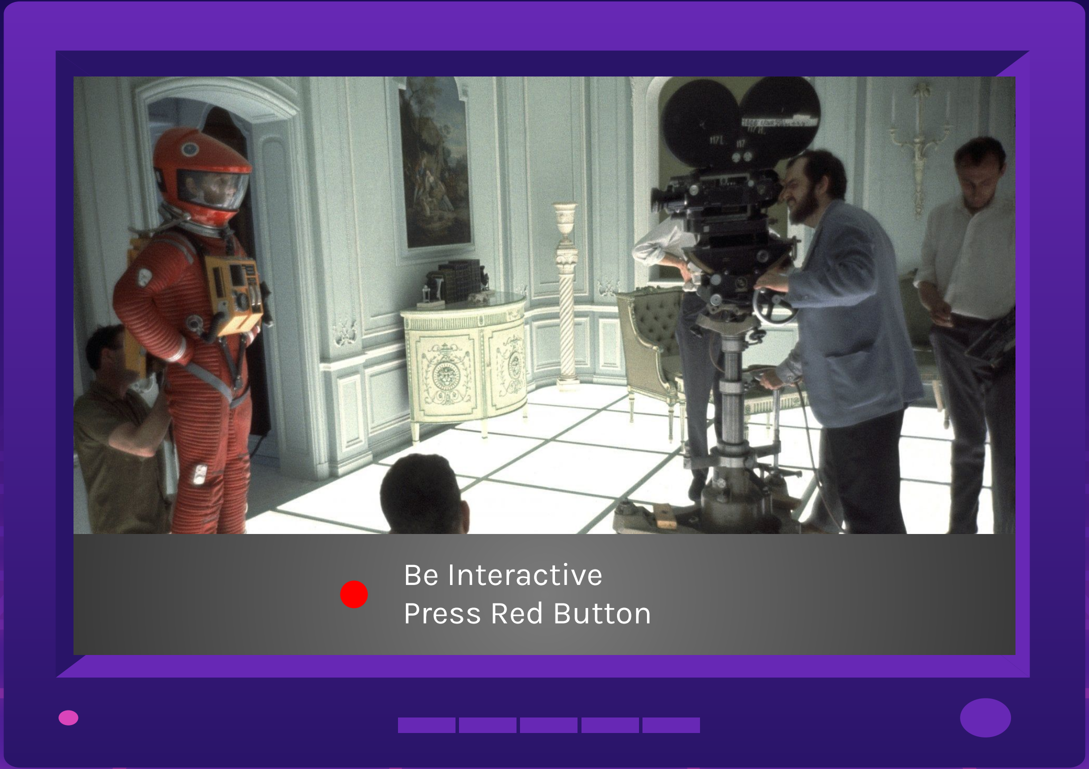
# Investigating HbbTV Privacy Invasiveness Across European Countries

Carlotta Tagliaro (TU Wien)

# Have you Ever Seen Such Banners?



● Be Interactive
Press Red Button

# Hybrid Broadcast Broadband TV

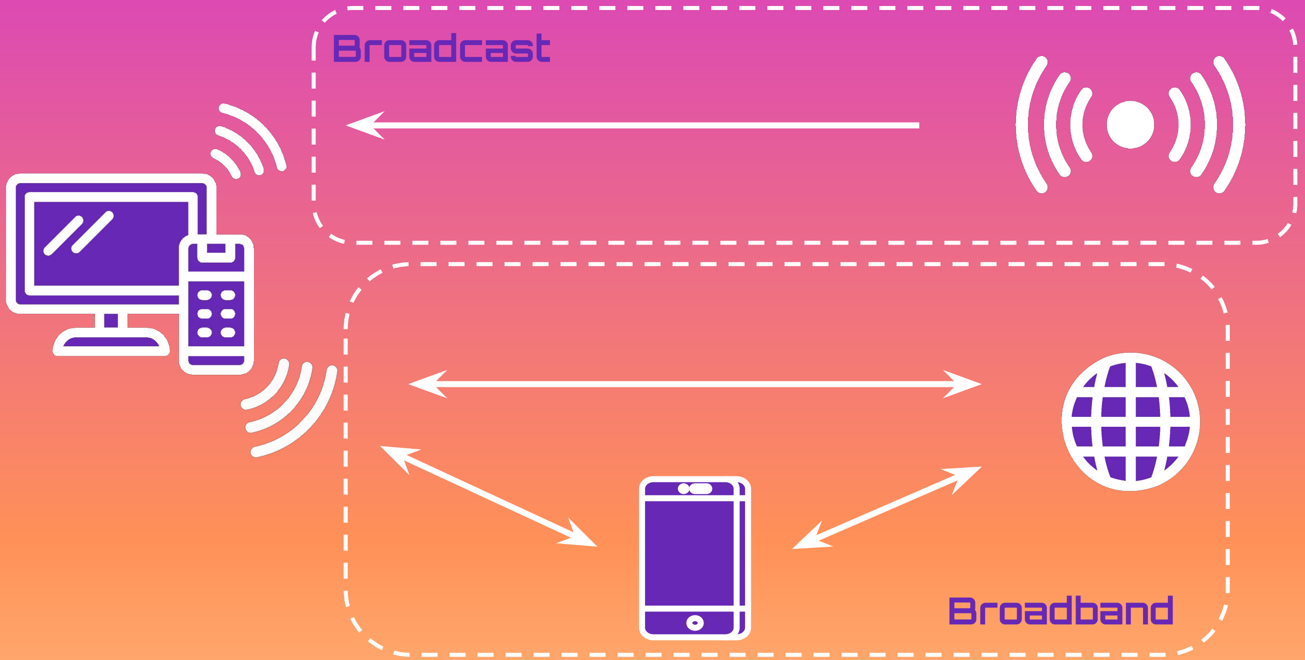
Initiative started in **2009** by an **industrial consortium** of industry leaders, e.g., German broadcaster RTL.

“**Harmonising the broadcast and broadband delivery of entertainment services** to consumers […].”

Two different connections:

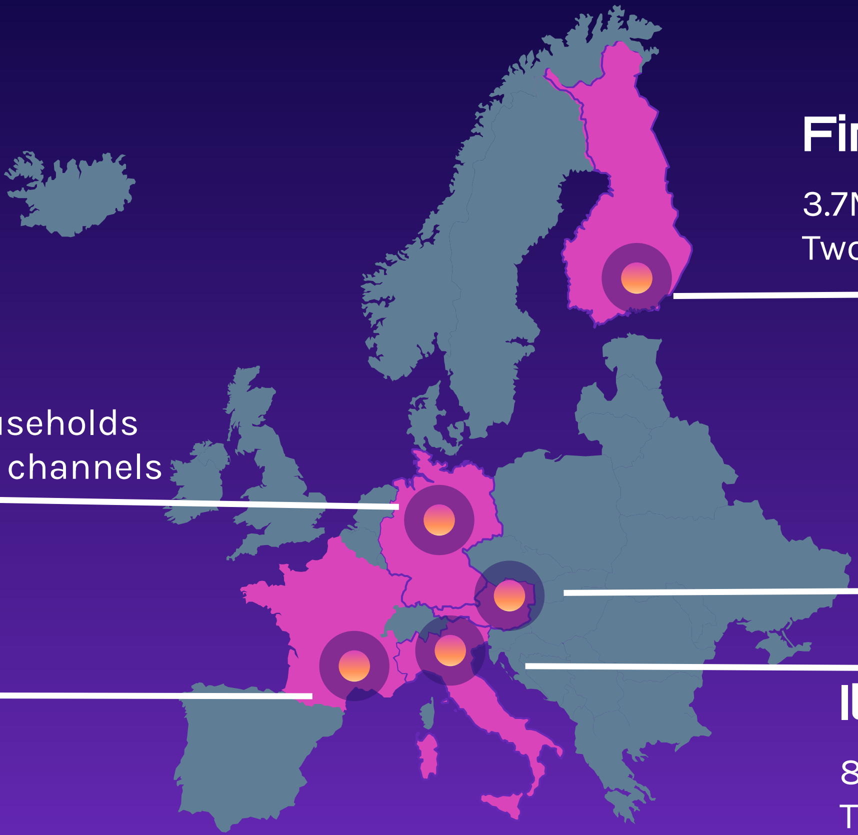
1. **Broadcast Digital Video Broadcasting (DVB)** network.
2. **Internet connection** via broadband interface.

HbbTV apps are **embedded as URLs in the DVB stream**, extracted and loaded in the **built-in TV browser** as **transparent graphical overlays**.



# HbbTV Architecture

# Analysis Across Five EU Countries



## Finland

3.7M HbbTV households
Two surveyed channels

## Germany

18M HbbTV households
Eight surveyed channels

## France

2.5M HbbTV households
Two surveyed channels

## Austria

1.4M HbbTV households
Four surveyed channels

## Italy

8.9M HbbTV households
Twenty surveyed channels

# Results

- In 26 channels trackers **before** users’ **consent.**
- 7 channels without **privacy policy**.
- Austria: all 4 channels contact ***track.tvping.com*** **every second** before consent.
- 20 channels use the **invisible “tracking pixel”** for profiling.
- German shopping channel HSE creates accounts over HTTP.

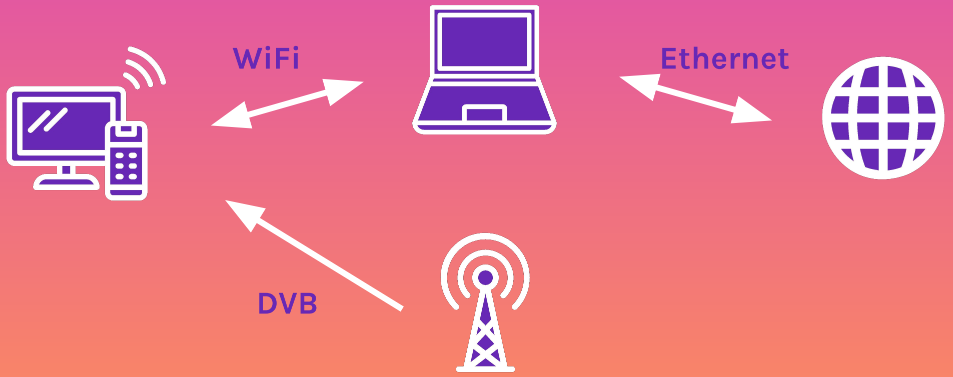
# Testing Equipment

- Two Smart TVs: a Xiaomi Mi 4A Smart TV (Android 9), and a Samsung M5500 Smart TV (Tizen 3.0).
    - Why two? Because some HbbTV applications were only working in the Samsung one!
- Laptop with Ubuntu 20.04.
- Antenna and UT-100c HiDes Modulator.
    - Modulator is needed to get broadcast signal and pass it to the laptop.
    - We choose a modulator supported by UNIX systems.
    - http://www.hides.com.tw/product_cg74469_eng.html

# Testing Methodology

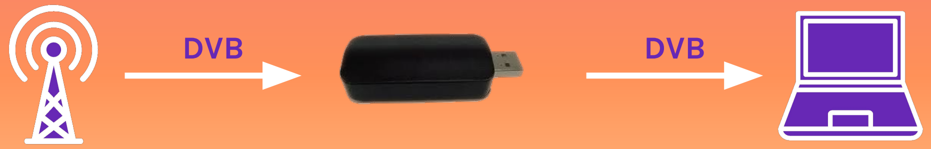
01

On-TV



02

Off-TV



# On-TV Traffic Inspection

Problem while capturing traffic generated by the TV:

**Encryption!**

How to bypass encryption?

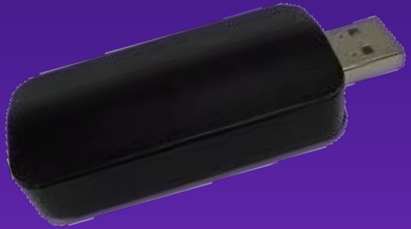
1. Proxy all TV traffic HbbTV traffic.
2. Make the TV trust the self-signed proxy CA.
3. Root access to write certificate in correct path.
4. Problems began!
   a. Magisk + Custom Recovery (TWRP).
   b. Privilege Escalation with Metasploit.
   c. ...

# Off-TV Traffic Inspection - I

Extract HbbTV URLs from DVB stream directly.

What we used:

- UT-100c HiDes Modulator.
- Antenna.
- TSDuck extensible toolkit for MPEG transport streams to parse DVB Stream.



# HiDes UT-100c

USB based modulator/demodulator with support for DVB-T transmission and reception.

Powered from the USB bus.

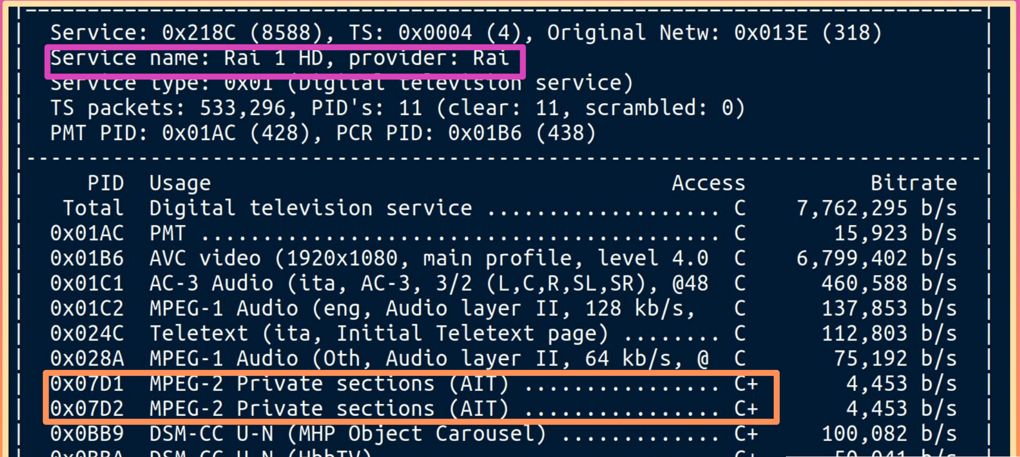
No host CPU computation required.

Price: US$169.

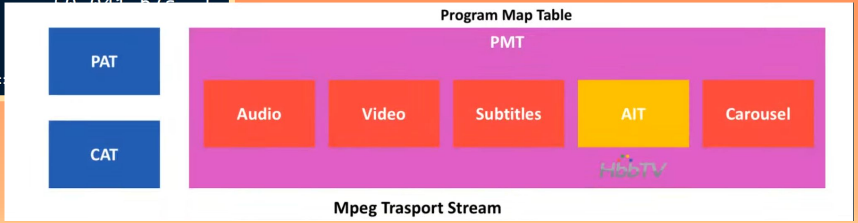
# Off-TV Traffic Inspection - II

1. Find the Ultra High Frequency of the channel.
2. Capture that specific UHF for 100 seconds.
3. Extract streams relative to Application Information Table.
4. Convert into XML to make it easily readable.
5. Open the files and look for code 0x0010 (HbbTV).
6. Get the URLs.

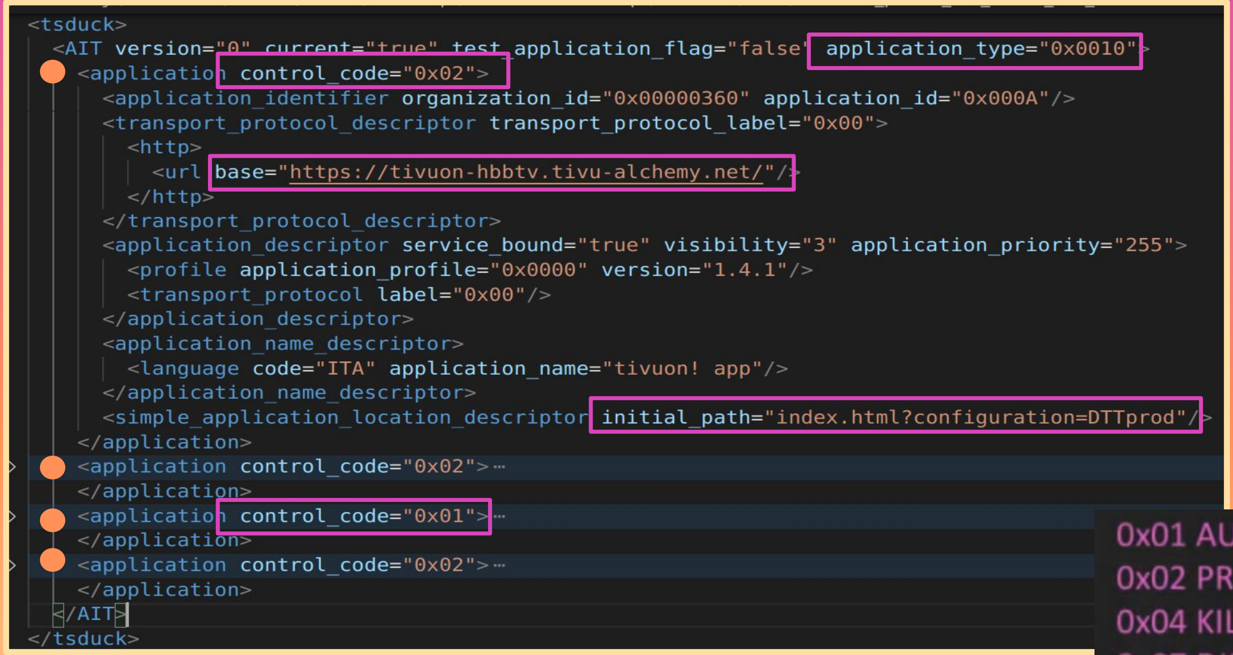
# Off-TV Traffic Inspection – III



```
|------------------------------------------------------------------------------|
|  Service: 0x218C (8588), TS: 0x0004 (4), Original Netw: 0x013E (318)         |
|  Service name: Rai 1 HD, provider: Rai                                       |
|  Service type: 0x01 (Digital television service)                             |
|  TS packets: 533,296, PID's: 11 (clear: 11, scrambled: 0)                    |
|  PMT PID: 0x01AC (428), PCR PID: 0x01B6 (438)                                |
|------------------------------------------------------------------------------|
|     PID  Usage                                  Access          Bitrate      |
|   Total  Digital television service ................... C    7,762,295 b/s  |
|  0x01AC  PMT ......................................... C       15,923 b/s  |
|  0x01B6  AVC video (1920x1080, main profile, level 4.0  C    6,799,402 b/s  |
|  0x01C1  AC-3 Audio (ita, AC-3, 3/2 (L,C,R,SL,SR), @48  C      460,588 b/s  |
|  0x01C2  MPEG-1 Audio (eng, Audio layer II, 128 kb/s,   C      137,853 b/s  |
|  0x024C  Teletext (ita, Initial Teletext page) ........ C      112,803 b/s  |
|  0x028A  MPEG-1 Audio (Oth, Audio layer II, 64 kb/s, @  C       75,192 b/s  |
|  0x07D1  MPEG-2 Private sections (AIT) ................ C+       4,453 b/s  |
|  0x07D2  MPEG-2 Private sections (AIT) ................ C+       4,453 b/s  |
|  0x0BB9  DSM-CC U-N (MHP Object Carousel) ............. C+     100,082 b/s  |
|  0x0BBA  DSM-CC U-N (HbbTV) ........................... C+      50,041 b/s  |
|  0x0C1D  DSM-CC Stream Descriptors .................... C+
|          (C=Clear, S=Scrambled, +=Shared)
|
==============================================================================
```



# Off-TV Traffic Inspection - IV



```
<tsduck>
  <AIT version="0" current="true" test_application_flag="false" application_type="0x0010">
    <application control_code="0x02">
      <application_identifier organization_id="0x00000360" application_id="0x000A"/>
      <transport_protocol_descriptor transport_protocol_label="0x00">
        <http>
          <url base="https://tivuon-hbbtv.tivu-alchemy.net/"/>
        </http>
      </transport_protocol_descriptor>
      <application_descriptor service_bound="true" visibility="3" application_priority="255">
        <profile application_profile="0x0000" version="1.4.1"/>
        <transport_protocol label="0x00"/>
      </application_descriptor>
      <application_name_descriptor>
        <language code="ITA" application_name="tivuon! app"/>
      </application_name_descriptor>
      <simple_application_location_descriptor initial_path="index.html?configuration=DTTprod"/>
    </application>
    <application control_code="0x02">⋯
    </application>
    <application control_code="0x01">⋯
    </application>
    <application control_code="0x02">⋯
    </application>
  </AIT>
</tsduck>
```

0x01 AUTOSTART
0x02 PRESENT
0x04 KILL
0x07 DISABLED

# Challenges Faced when Extracting URLs

1. Antenna not strong enough to capture broadcast signal for all channels.

2. Some countries only adopt cabled signal.

24 successfully extracted HbbTV apps (out of 36 channels).

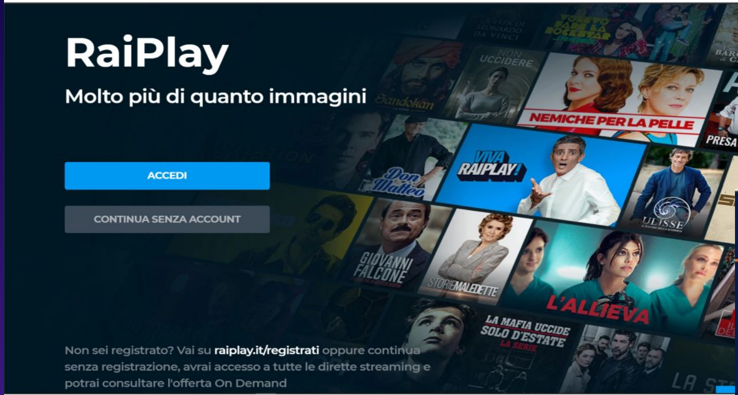
Foster reproducibility and flexibility of testing (URLs can be tested from anywhere).

# Open URLs in Browser

Open the HbbTV URLs in laptop’s browser:

1. Some detect that User-Agent is not from a Smart TV: We custom change it.
2. In some cases, use a Smart TV browser emulator to bind the key events, playback mp4 videos and simulate embedded broadcast signal (RedOrbit HbbTV Emulator).

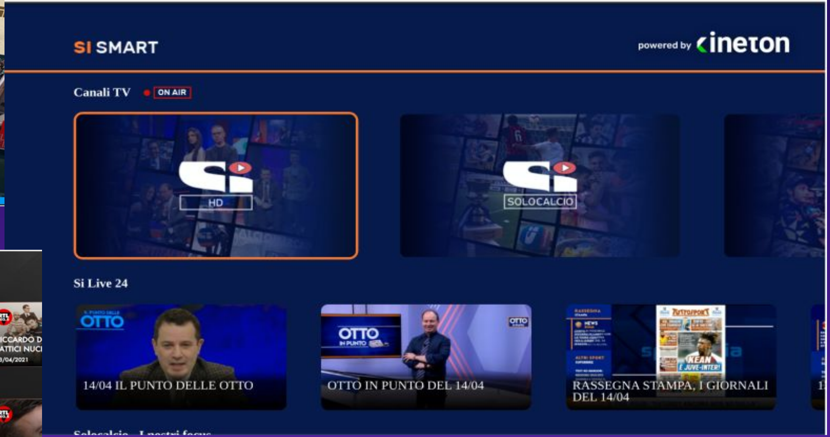
# Examples of HbbTV Apps

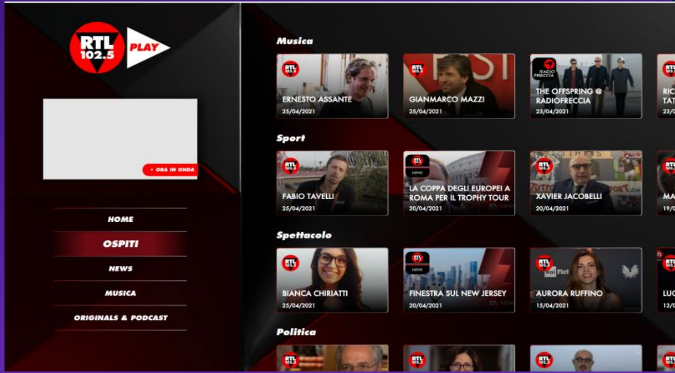


RaiPlay

Molto più di quanto immagini

Non sei registrato? Vai su **raiplay.it/registrati** oppure continua senza registrazione, avrai accesso a tutte le dirette streaming e potrai consultare l'offerta On Demand





RTL 102.5 PLAY
ORA IN ONDA
HOME
OSPITI
NEWS
MUSICA
ORIGINALS & PODCAST
Musica
ERNESTO ASSANTE 25/04/2021
GIANMARCO MAZZI 25/04/2021
THE OFFSPRING @ RADIOFRECCIA 23/04/2021
Sport
FABIO TAVELLI 25/04/2021
LA COPPA DEGLI EUROPEI A ROMA PER IL TROPHY TOUR 20/04/2021
XAVIER JACOBELLI 20/04/2021
Spettacolo
BIANCA CHIRIATTI 25/04/2021
FINESTRA SUL NEW JERSEY 20/04/2021
AURORA RUFFINO 15/04/2021
Politica

# Traffic Capture Phases - I

Traffic capture divided into four phases:

1. **Before consent:**
   - Privacy notice about data treatment.
   - No communication should take place.
   - No tracking domains.
2. **Interaction:**
   - Accept privacy policy (if present).
   - Interact with the apps' buttons.

# Traffic Capture Phases - II

3. **Consent Revocation**:
    - Revoke consent.
    - Cookies must be deleted.
    - Tracking must stop.
4. **Consent Again**:
    - Change channel and Retune.
    - Check cookies (if same ones or different from 2.).

Same approach for all the countries with unique testing procedure that can be replicated by researchers.

# Parsing of Traffic Files

Traffic captured in PCAPs. With TShark We extract:

1. Domain name.
2. Testing phase where domain is found (“before-consent”, “after-consent”, “consent-revoked”, “consent-restored”).
3. Number of requests to that host.
4. If HTTP or HTTPS traffic.
5. Returned object type (if any).
6. Cookies that have been set and their expiration dates.

# Automation and Manual Effort

Automate as much as possible to avoid imprecisions:

- Precisely time capture phases via Wireshark.
- Extraction of domains from PCAPs.

BUT automation not always possible:

- Manually search the scope of domains (e.g., tracking, content providers) and who they belong to.
  - Matching domains against existing tracking deny-lists not enough.
- Interaction with HbbTV apps.

# Survey and Ethical Considerations

Follow ethical guidelines defined by our university.

Before starting the survey, receive approval from the ethical committee.

On the first page of the questionnaire, our contact information.

Participation is voluntary, and the survey can be stopped at any point.

Inform participants what data will be collected and how it will be used.

# Adopted Survey Platform

Platform **soscisurvey.de:**

- highly customizable:
  - Risky scenarios displayed in random order for each participants.
  - Show some questions only if others were completed.
- Hosted in Germany.
- Data are stored in the EU (subject to GDPR).

# Survey Methodology

Mixed-method design approach:

- **Quantitative**:
  - Closed questions (multiple- or single-choice) to gather general statistics.
  - Examples: age, whether participants own or not a Smart TV.
- **Qualitative**:
  - Open-ended questions.
  - Simulate an interview by asking the participant to resonate.
  - Open coding approach to cluster open-ended responses.

# What Did We Borrow? - I

Previous related work by Ghiglieri et al.

- TV Experiments:
  - Only on German channels: we expand to four other countries.
  - Four testing phases are the same for comparability.
  - Dated 2013-2015: results now outdated we capture traffic in 2021/2022 with HbbTV newer 2.0 version.
  - Mostly HTTP traffic: we see more use of encryption and develop the Off-TV testing procedure to bypass it.

# What Did We Borrow? - II

- Awareness Survey:
  - Similar approach but more targeted to HbbTV.
  - We send the survey to Italian consumers while it was first conducted over German ones.

Measurement papers tend to outdate quickly; results from five years ago do not depict current HbbTV situation.

Interesting to find that German channel HSE still sends credit card details and account information over HTTP.

# Open Challenges

1. Bypassing encryption when performing On-TV tests.
    a. Rooting the Smart TV.
    b. Install proxy CA certificate.
2. Extract HbbTV URLs when no antenna signal present.
3. Properly handle HbbTV apps in TV browser simulated environment.
4. Gather more survey participants to avoid biases.

# What's Next?

1. Disclosure process; currently trying to contact CERTs from different countries without much success.

2. Test the adoption of HbbTV in different European countries and for more channels.

3. Investigate the Samsung/Android apps' incompatibility.

4. Study the adoption of similar protocols in non-EU countries, e.g., the US.

# Thank you!

## Any questions?

Presenter: Carlotta Tagliaro
Email: carlotta@seclab.wien
Twitter: @Pseudorandomico

GitHub repo: https://github.com/SecPriv/hbbtv-blocker

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik and illustrations by Stories.