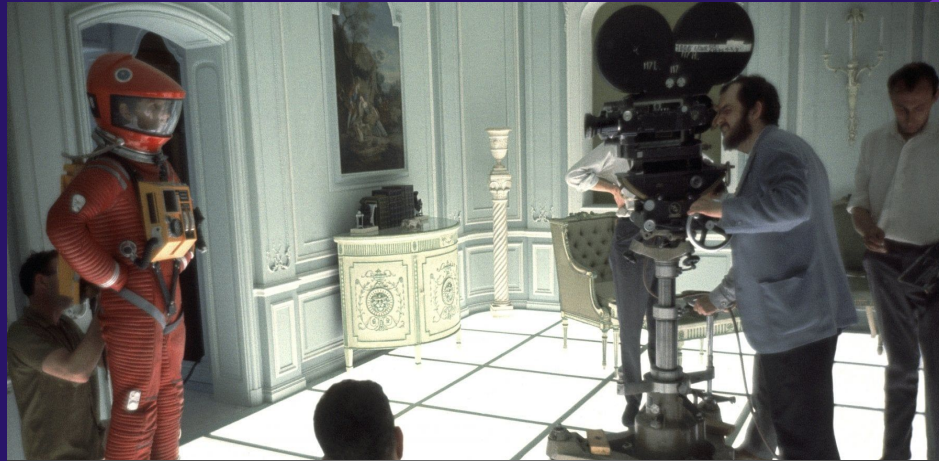


I Still Know What You Watched Last Sunday

Privacy of the HbbTV Protocol in the European Smart
TV Landscape

Carlotta Tagliaro (TU Wien), Florian Hahn (University of
Twente), Riccardo Sepe (Guess Europe), Alessio Aceti
(Sababa Security), Martina Lindorfer (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.

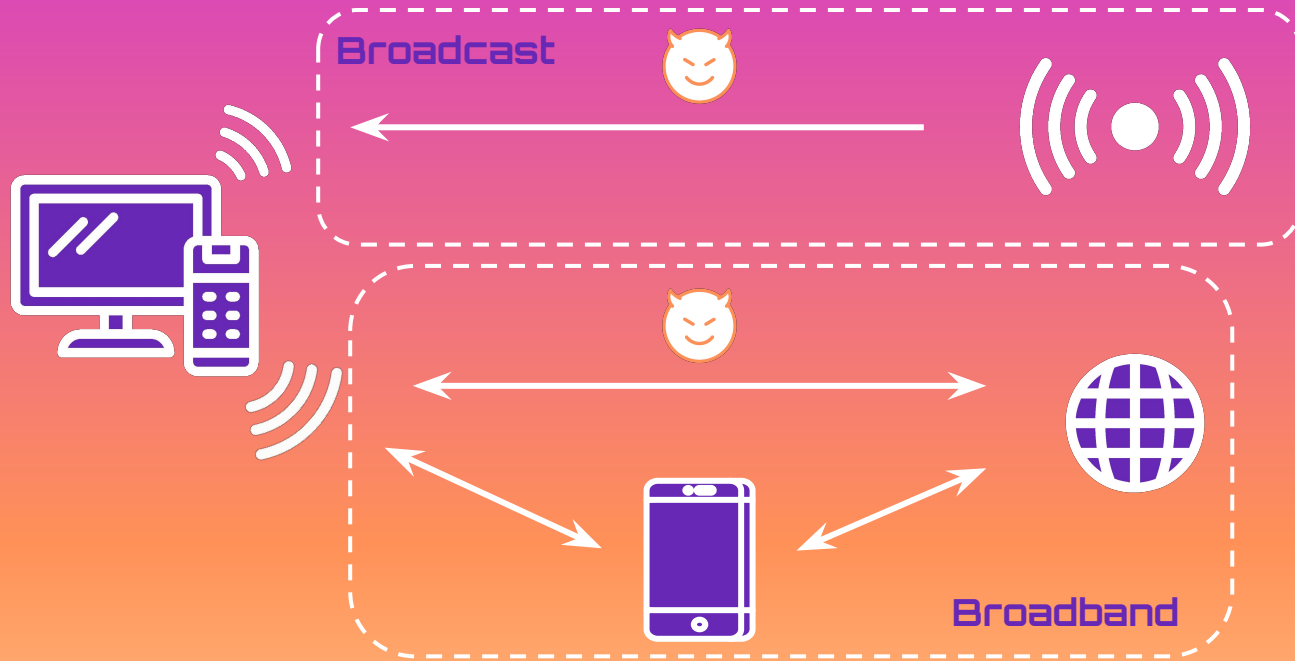
“**Harmonising the broadcast and broadband delivery of entertainment services** to consumers [...]”

Two different connections:

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

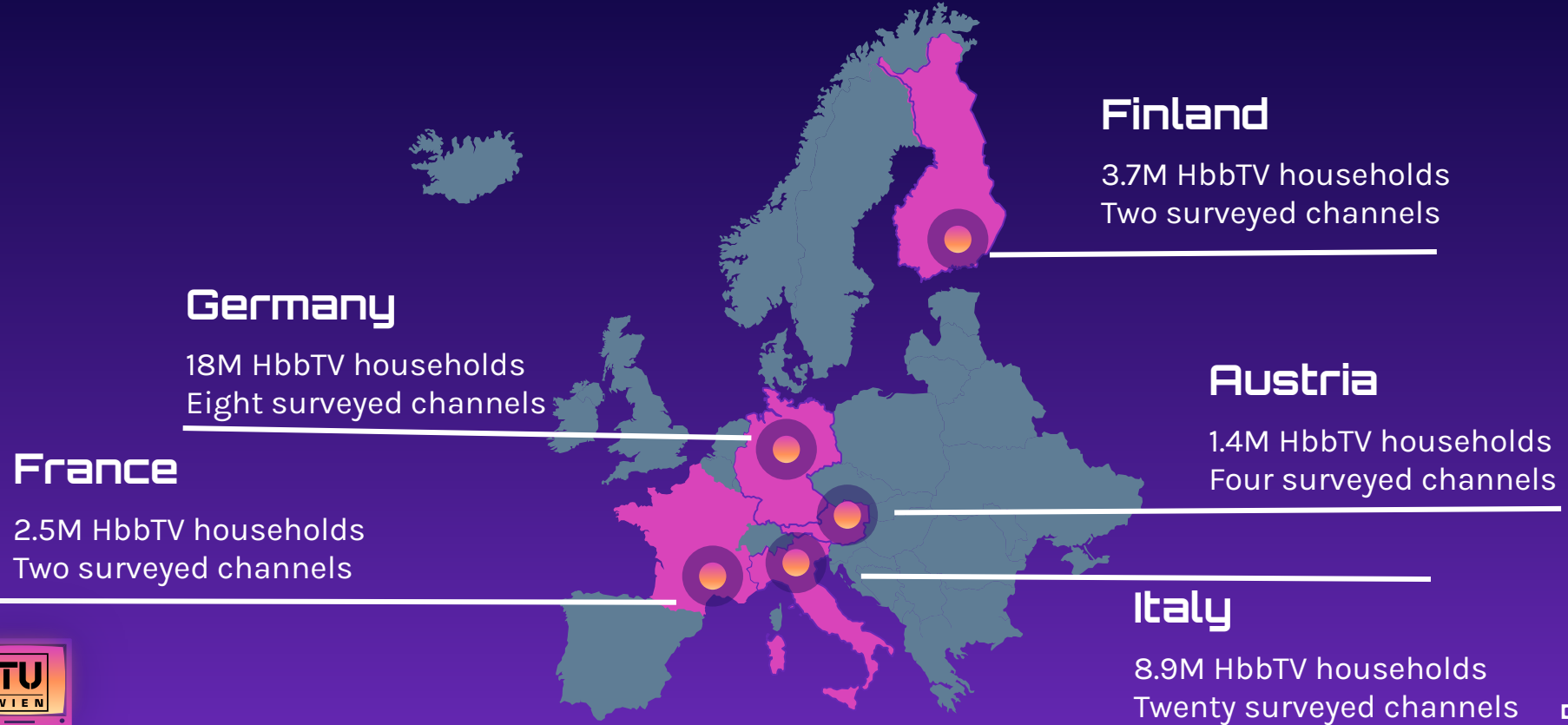
HbbTV apps are **embedded as URLs in the DVB stream**, extracted and loaded in the **built-in TV browser** as transparent **graphical overlays**.





HbbTV Threat Architecture

Analysis Across Five EU Countries



Germany

18M HbbTV households
Eight surveyed channels

Finland

3.7M HbbTV households
Two surveyed channels

Austria

1.4M HbbTV households
Four surveyed channels

France

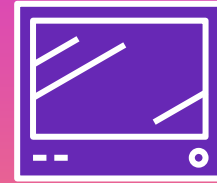
2.5M HbbTV households
Two surveyed channels

Italy

8.9M HbbTV households
Twenty surveyed channels



On-TV Traffic Inspection



We record traffic for **one hour** in **four phases**:

1. Listen for 15 minutes **without** any **interaction**.
2. **Give consent** and interact for 20 minutes with the buttons.
3. **Revoke consent** and listen for 10 minutes without interaction.
4. **Restore consent** and listen for 15 minutes.

Factory reset for each channel analysis.

We adapted the approach from Ghiglieri et al. [1]

[1] https://www.ieee-security.org/TC/W2SP/2014/papers/ghiglieri_hbbtv%20survey.pdf

Off-TV Traffic Inspection - I



We extract the HbbTV URLs from the DVB stream using the **TSDuck library** and the **UT-100c HiDes modulator**.

We open the URLs in a browser, **mimicking the Smart TV environment**. We bypass the limitations of encryption.

We capture only **30 minutes of traffic** with the same **four phases**.

Off-TV Traffic Inspection - II



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
Total	Digital television service	C
0x01AC	PMT	C
0x01B6	AVC video (1920x1080, main profile, level 4.0	C
0x01C1	AC-3 Audio (ita, AC-3, 3/2 (L,C,R,SL,SR), @48	C
0x01C2	MPEG-1 Audio (eng, Audio layer II, 128 kb/s,	C
0x024C	Teletext (ita, Initial Teletext page)	C
0x028A	MPEG-1 Audio (Oth, Audio layer II, 64 kb/s, @	C
0x07D1	MPEG-2 Private sections (AIT)	C+
0x07D2	MPEG-2 Private sections (AIT)	C+
0x0BB9	DSM-CC U-N (MHP Object Carousel)	C+
0x0BBA	DSM-CC U-N (HbbTV)	C+
0x0C1D	DSM-CC Stream Descriptors	C+

(C=Clear, S=Scrambled, +=Shared)

```
<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=DTIprod"/>
  </application>
  <application control_code="0x02">
  </application>
  <application control_code="0x01">
  </application>
  <application control_code="0x02">
  </application>
</AIT>
</tsduck>
```


Wait a Minute! What is This?

```
10.42.0.244
scheduler.hbbtv.smartclip.net
10.42.0.244
scheduler.hbbtv.smartclip.net
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
scheduler.hbbtv.smartclip.net
10.42.0.244
scheduler.hbbtv.smartclip.net
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
10.42.0.244
track.tvping.com
```



Whoa!
The TV is
Tracking
us!



Consent

- 26 communicate with trackers **before users' consent.**
- 7 channels do not present **any privacy policy.**
- For Austria, all 4 channels contact ***track.tvping.com* every second** before consent.

- All 36 channels contact at least one tracking domain.
- 20 channels adopt the invisible “tracking pixel” for profiling by uploading a 1x1 pixel image.





Use of HTTP

- HTTP in 24 channels with sensitive information such as **device/visitor IDs, country, and ISP information.**
- The German **shopping channel HSE** allows to create **accounts over HTTP**, exposing credentials and credit card data.

GDPR Violations & Security Risks

- **Tracking before consent** contradicts the “**Conditions for Consent**”.
- **Withdrawing consent**, with the deletion of data, **must be possible**.
- The **absence and incorrectness of the privacy notice** violates **transparent communication and provision of correct information**.

Online shopping apps via HbbTV exist. Sensitive data such as credit card information is inserted. The **incorrect handling leads to severe security issues**.

Users' Awareness Survey: are Consumers Aware of the Risks?

01

Awareness of
Security and
Privacy Risks

02

Risk
Assessment of
Scenarios

03

Privacy Policy

04

Preferred Mode
of TV
Connection



Users' Awareness

- 68%: could not mention any risk.
- 68%: never read privacy policies presented by digital services.
- Average risk score ranges from **2.70** to **3.97**; highly concerned with their security and privacy but **unaware of the risks.**

Any questions?



Thank
you!

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.



HbbTV Blocker: an initial step towards a private viewing experience

Gateway-based.

Default private configuration working out of the box.

Per-Channel Denylist.

Check for new tracking domains using the most recent PiHole and EasyList lists.

Graphical dashboard to allow configuration.

