# I Still Know What You Watched Last Sunday: Privacy of the HbbTV Protocol in the European Smart TV Landscape

Carlotta Tagliaro
TU Wien
Austria
carlotta@seclab.wien

Florian Hahn
University of Twente
Netherlands
f.w.hahn@utwente.nl

Riccardo Sepe
Guess Europe Sagl
Italy
riccardo@sepe.it

Alessio Aceti
Sababa Security SpA
Italy
alessio.aceti@sababasecurity.com

Martina Lindorfer
TU Wien
Austria
martina@seclab.wien

***Abstract*—The ever-increasing popularity of Smart TVs and support for the Hybrid Broadcast Broadband TV (HbbTV) standard allow broadcasters to enrich content offered to users via the standard broadcast signal with Internet-delivered apps, e.g., ranging from quizzes during a TV show to targeted advertisement. HbbTV works using standard web technologies as transparent overlays over a TV channel. Despite the number of HbbTV-enabled devices rapidly growing, studies on the protocol's security and privacy aspects are scarce, and no standard protective measure is in place.**

**We fill this gap by investigating the current state of HbbTV in the European landscape and assessing its implications for users' privacy. We shift the focus from the Smart TV's firmware and app security, already studied in-depth in related work, to the content transmission protocol itself. Contrary to traditional "linear TV" signals, HbbTV allows for bi-directional communication: in addition to receiving TV content, it also allows for transmitting data back to the broadcaster. We describe techniques broadcasters use to measure users' (viewing) preferences and show how the protocol's implementation can cause severe privacy risks by studying its deployment by 36 TV channels in five European countries (Italy, Germany, France, Austria, and Finland). We also survey users' awareness of Smart TV and HbbTV-related risks. Our results show little understanding of the possible threats users are exposed to. Finally, we present a denylist-based mechanism to ensure a safe experience for users when watching TV and to reduce the privacy issues that HbbTV may pose.**

## I. Introduction

As of 2021, 1.72 billion TV households exist worldwide [82], and each viewer, on average, spends around three hours per day watching TV [77], [80]. Thus, TV content can significantly impact society as a whole, for example, depending on the content and spin of news headlines—in addition to being a valuable target for advertisers. However, traditional "linear TV" (i.e., content that is broadcasted as scheduled programs, including commercial breaks) through satellite or cable has faced stiff competition from new on-demand streaming services, like Netflix, Hulu, HBO Max, Amazon Prime Video, and Apple TV+.

Thus, to combine standard TV's broadcast content delivery with the powerful digital content delivery of the new platforms and improve the viewing experience for users, an industrial consortium launched the *Hybrid Broadcast Broadband TV (HbbTV)* [16] initiative in 2009. HbbTV sets a standard for a broadcast/broadband hybrid protocol to deliver content to Smart TVs, set-top boxes, and other connected multiscreen devices in an interconnected environment. In this setting, an HbbTV application is loaded and executed by a Smart TV's built-in browser and displayed as a graphic overlay on top of regular broadcast content. In addition, HbbTV transforms the traditional TV viewing experience from merely *receiving* content to also *transmitting* data, enabling new functionality for users (e.g., interactive programming and shopping) and broadcasters (e.g., measuring viewing preferences).

The adoption rate and support of HbbTV have been growing steadily. As of 2022, HbbTV has been adopted across European countries, as well as Australia, Russia, and Vietnam [8]. Germany represents the leading country in HbbTV adoption and was the first to adopt this standard: over 90% of Smart TVs sold support the HbbTV standard [8]. Looking at the general HbbTV adoption in the European countries we focus on, compared to the general numbers of TV households (i.e., households with a TV set), 8.95 million out of 25 million (44.75%) in Italy, 2.5 million out of 28.8 million (6.68%) in France, and 18 million out of 38.52 million (46.73%) in Germany have HbbTV-enabled devices [8], [55], [48].

Thus, differently from previous work that studied security and privacy aspects of the Smart TV's firmware and apps, we focus on the transmission protocol itself. Recent studies have already shown that HbbTV provides users little or no security and privacy. Most notably, Ghiglieri et al. [45], [46], [47], [44] assessed HbbTV's privacy posture highlighting the severe risks users were exposed to. Additionally, little or no control is given to the viewer; they have no means to detect whether a connection is secured, which data is transferred, and how it is used. HbbTV's security and privacy issues are manifold. They range from a simple echo request from the broadcaster to check if the user is still watching to content-based attacks that replace URLs to show viewers different content than was intended. These issues have also been abused in practice, most recently in May 2022 when hackers exploited HbbTV broadcasts of Russian TV stations to show anti-war messages [51].

Network and Distributed System Security (NDSS) Symposium 2023
27 February - 3 March 2023, San Diego, CA, USA
ISBN 1-891562-83-5
https://dx.doi.org/10.14722/ndss.2023.24102
www.ndss-symposium.org

When combining the insecurities of the HbbTV protocol with tracking and data analytics, users' privacy is even at greater risk: TV viewing behavior provides "very detailed and sensitive insights into what users think, know and believe" [52]. A new form of advertisements (ads) aims to mine this data and take advantage of the dynamic content delivery through HbbTV: *Addressable TV (ATV)*. With ATV, the static delivery of ads over the standard broadcast signal is expected to be replaced by dynamic ad insertion, i.e., instead of all viewers of a TV program seeing the same ads during commercial breaks, targeted ads can be delivered over the Internet [76], [55]. Thus, ATV might increase privacy risks for TV consumers. Several companies have recently developed new solutions to collect and analyze data for ATV, ranging from Smartclip, over Equifax, to Castoola [55], [4], [7]. Furthermore, the numerous players in the Smart TV ecosystem and the scattered and outdated legal framework create additional complexity in data handling [41].

Some solutions to protect users' privacy in the Smart TV domain are already available, such as DNS blocking of tracking domains [85], [45], [59]. However, they are not sufficient, since they either block all incoming traffic, or rely on incomplete and, thus, ineffective denylists. In general, most solutions are not yet designed to address TV tracking. Furthermore, the (Smart) TV landscape is rapidly changing. The HbbTV protocol itself is improving with a shift towards HbbTV 2.0 with new security measures (e.g., increased use of HTTPS over HTTP). Thus, in this paper, we revisit and extend previous studies on the privacy posture of HbbTV in light of protocol changes and increased adoption. We start by studying how the TV landscape has changed after the more widespread adoption of HbbTV to see if broadcasters take better care of users' privacy by looking at the traffic between a Smart TV and the servers offering HbbTV applications. In particular, we focus on Italy, Germany, France, Austria, and Finland, countries that (1) are actively adopting the HbbTV [8] and (2) are known for strong awareness and support for privacy and data protection regulations [39], [42]. In these countries, we perform active measurements on 36 different TV channels using both Smart TVs and off-device protocol inspection to investigate privacy aspects of the channels' HbbTV implementation in 2021 and 2022. We complement these experiments by studying whether users have become more security and privacy aware after being more frequently exposed to HbbTV applications.

In summary, our main contributions are as follows:

- We show little progress in the protection of data sent between broadcasters and Smart TVs over the years: Users are still exposed to privacy risks, such as tracking before expressing consent and the transmission of credit card details through insecure plaintext traffic.
- We investigate users' privacy and security awareness, showing a general lack of knowledge of HbbTV's risks. We also show great concern for their data when confronted with risks linked to Smart TVs and HbbTV.
- Based on the results of our technical and qualitative analysis, we design an "HbbTV Blocker" to intercept and block unwanted traffic from the Smart TVs to the broadcasters (and vice versa).

**Responsible Disclosure.** We put particular care into identifying problems concerning users' privacy in light of current legislation: (1) The *General Data Protection Regulation (GDPR)*, which has been effective since 2018 to protect European citizens' data and privacy [12], and, given the geographical setting of our analysis, (2) the *Garante per la Protezione dei Dati Personali (GPDP)* [11], the Italian administrative authority for data protection (see Section VIII).

We are working with the GPDP and the Computer Emergency Response Team Austria (CERT.at) [27] to responsibly disclose the issues found to the broadcasters. We will provide updates on the outcome of this process in the repository below.

**Artifacts.** The source code of our experiment setup, the HbbTV Blocker, and the collected denylist of tracking domains are available at https://github.com/SecPriv/hbbtv-blocker.

## II. Background

### A. Hybrid Broadcast Broadband TV (HbbTV)

**HbbTV Specification.** HbbTV, as stated by the HbbTV Association [16], is "... a global initiative aimed at harmonizing the broadcast and broadband delivery of entertainment services to consumers through connected TVs, set-top boxes, and multiscreen devices." In other words, it represents both a widely adopted standard (the ETSI Technical Specification 102 796 [40]), and a driving force to promote a unified hybrid TV delivery across different platforms [34] offering broadcast and broadband content to viewers. The initiative dates back to 2009 when a group of industry leaders, led by the German broadcaster RTL, introduced a different form of Teletext using HbbTV and the CE-HTML interface language, an XHTML-based standard for websites with remote user interfaces typically used in consumer electronic devices.

The HbbTV standard works either via broadcast or via IP link; however, it is most powerful in an Internet-connected environment where a combination of broadcast and broadband networking can deliver additional content to the user. For HbbTV to work, the TV must support it, and then the broadcaster must provide at least one HbbTV application for the user to interact with. When such an application is delivered to the user, they are typically informed that some extra HbbTV content is available with a relevant icon. Such additional information can be in the form of program guides, viewer interaction (e.g., with quizzes during a show), lyrics of music videos, additional advertising, and customized content.

To interact with such extra content, until HbbTV version 1.5, the user could use the Smart TV remote control, more specifically through the colored buttons. Instead, HbbTV 2.0 offers the possibility of connecting different devices, such as smartphones and tablets, allowing multi-device interactions.

Unlike the Internet Protocol TV (IPTV), HbbTV still relies on the standard broadcast signal to deliver the initial application URL and launch it as an overlay on top of standard TV. It does not represent an alternative way to receive content but rather an enhanced version. Additionally, HbbTV, except for premium features, is free for the user; instead, to benefit from IPTV, users typically have to pay a subscription fee. Those two considerations combined make HbbTV more appealing to advertisers and trackers who can reach a greater audience.

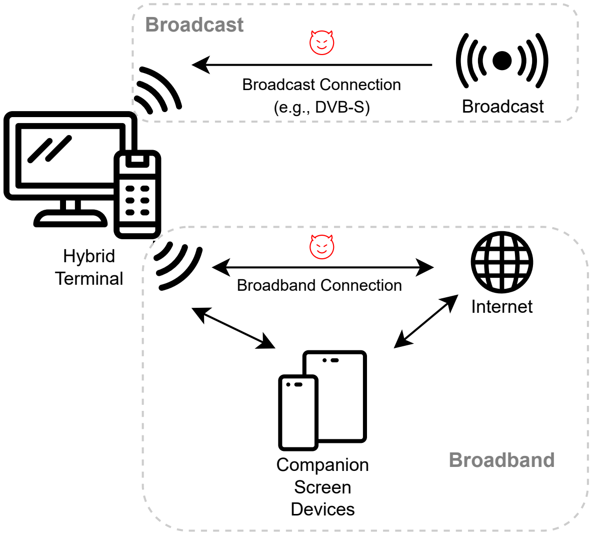

Fig. 1. HbbTV System Overview: The hybrid terminal represents a Smart TV with dual connection (i.e., broadband and broadcast). We highlight the attack channels we focus on during the remainder of our paper.

**HbbTV Communication.** A Smart TV (i.e., a hybrid terminal) can support two different connections in parallel; on one side, it is connected to a broadcast Digital Video Broadcasting (DVB) network. On the other side, it is connected to the Internet via a broadband interface. The TV receives standard broadcast Audio/Video (A/V) content through the first one and allows for the signaling of stream events to an application. The Internet connection allows for bi-directional communication with the provider and can receive non-linear A/V content. The broadband interface may also connect with other HbbTV terminals or "Companion Screen Devices" (e.g., smartphones and tablets) on the same local network. We show the interaction between the different actors in Figure 1.

Through the Broadcast interface, the terminal also receives application data and stream events that are transferred using Digital Storage Media - Command and Control (DSM-CC) objects. Non-realtime content is transmitted using the File Delivery Protocol (FDP) protocol. The data is sent to the Runtime Environment of the terminal composed of the Application Manager, the Browser, and the Companion Screen Interface. Via the Broadband interface, the Smart TV also connects to the Internet. This connection provides a way to request application data from a provider's servers. Data collected in this way is again transferred to the Runtime Environment [49].

**The TV as a Browser.** The Internet-delivered HbbTV applications are embedded as URLs in the DVB stream sent by broadcasters. The Internet Protocol Processing component parses the data from the Internet and passes the information to the Runtime Environment. This environment includes the TV's browser, responsible for presenting and executing the application. Any website written with standard web techniques (e.g., HTML, CSS, JavaScript) can serve content. When the application is loaded, the browser displays a notification overlay to the user showing that the application is ready to be activated through the remote control (via the standard *Red Button*).

### *B. Security & Privacy Concerns with HbbTV*

Despite statistics showing an ever-increasing adoption of HbbTV, little or no literature is available on its security and privacy issues. Up to now, the main focus of researchers has been vulnerabilities linked to physical access to such devices either through the USB port or local network [75], [71], [50]. However, as mentioned above, Smart TVs that support HbbTV can access online content and websites through the integrated web browser—opening up a plethora of different attacks. Before delving into the details of potential attacks, it is worth mentioning that the HbbTV specification presents a security-related chapter. It states that the user shall trust only broadcast-related applications and not broadcast-independent ones. However, it does not mention how to perform such a control, and additionally, the user can bypass such a restriction by making broadcast-independent applications trusted.

**Encryption and Certificates.** On the broadband side, the HbbTV specification mentions that security is provided by adopting the Transport Layer Security (TLS) protocols. The standard presents several requirements concerning the adoption of TLS, such as the supported cipher suites, the minimal key length, and the forbidden use of compression algorithms. At the same time, adopting TLS (or, more specifically, HTTP over TLS (HTTPS)) is strongly suggested; whether it is implemented depends on device manufacturers and the actors delivering content to the user [49].

**Privacy and Tracking.** The standard allows the user to specify their tracking policy by choosing between two alternatives: Do Not Track (`DNT`) set to 1, i.e., no tracking consent, or set to 0, i.e., tracking consent. To explicit user's tracking preferences, the `DNT` parameter is included in every outgoing HTTP request. However, again, in this case, it is up to application developers and device manufacturers to correctly implement this. Several problems might arise if tracking websites are allowed, especially in autostart applications (i.e., applications that run without the user knowing and without the need for their consent) or even if persistent cookies are stored. Persistent cookies remain until the expiry date and, as reported in Section III, can be highly problematic since the date set is far in time, allowing tracking over a long period [49].

As previously described, most HbbTV apps run in a built-in browser that displays HTML content and runs JavaScript code. The DVB stream contains the HbbTV URL (retrieved from specific web servers) that is opened in the browser and shown as a semi-transparent HTML layer that overlaps the actual TV program. In such a way, the TV becomes visible to the broadcaster even before the user consents to it, possibly breaching their privacy. We report more details in Section III.

As with other web content delivered to desktop and mobile browsers, third-party tracking represents a problem in this scenario. A study conducted in 2013 over 66 different German stations showed that 13 among them used Google Analytics to track users [50]. This could not only impact users' privacy, but an attacker can exploit such a feature to spam fake analytics via proxy networks simulating actual TVs and influence broadcasters' decisions, e.g., to discontinue a specific show.

### *C. Threat Model*

In our threat model, the Smart TV is connected to the Internet. The broadcaster communicates with the device over traditional broadcast and broadband signal. We identify two potential threat actors. The first is an ill-intentioned broadcaster that tracks users' preferences and viewing times without asking for their consent via cookies and by sending profiling data over HbbTV. This data can later be used to show targeted and personalized advertisement mining users' autonomy. More generally, the broadcaster and any party providing HbbTV content such as included advertisers and trackers can compromise users' privacy either on purpose or through misconfiguration and negligence. The second threat actor is represented by anyone who has access to the traffic generated by the TV (e.g., an Internet provider or an actor connected to the same network) that can intercept unencrypted HTTP traffic, possibly sniffing sensitive information such as usernames and passwords.

## III. RELATED WORK

**Smart TV and IoT Security.** Weak certificate validation is a known issue with Smart TVs. Paracha et al. show that most IoT devices (including Smart TVs) implement TLS incorrectly, using deprecated ciphers, not correctly validating certificates, or containing deprecated root certificates [66]. Aafer et al. assessed the security level of Android TV boxes by fuzzing target vendors' APIs, finding 37 unique vulnerabilities [28]. Bachy et al. showed the feasibility of attacks via local loops supporting the ADSL network and DVB, finding several security vulnerabilities. They also report different techniques for extracting and analyzing the firmware of Smart TVs [31]. Moghaddam et al. investigated the privacy of two OTT devices, Amazon Fire TV and Roku TV, showing that, respectively, 89% and 69% of the top 1,000 viewed channels for each platform contact at least one tracking domain even when the user explicitly selects the enhanced privacy feature [62]. In addition, an attacker can use the Smart TV as a starting point to access the user's private WiFi network. Barre et al. demonstrated the feasibility of using the Smart TV as a relay to attack further devices [32]. Acar et al. showed how machine learning techniques could help identify IoT devices (potentially including Smart TVs) only by passively listening to network traffic [29]. Puche Rondon et al. investigated Enterprise Internet-of-Things (E-IoT) showing that despite its "secure" reputation, several issues are present mining users' privacy and security [73] and also investigated one High Definition Multimedia Interface (HDMI) component, the Consumer Electronics Control (CEC) protocol, that takes an important role in receiving A/V content [72]. Instead of studying issues related to specific Smart TVs and local connections, our work focuses on issues in the HbbTV content delivery protocol used by broadcasters.

**HbbTV Security and Privacy.** Several proof-of-concept attacks showed HbbTV's susceptibility to content injection. In 2014, Oren and Keromytis manipulated an HbbTV URL at the DVB level, causing several devices to receive malicious content [65]. An attacker can exploit DVB/DSM-CC injection to replace content into streams, directly specifying the URLs pointing back to their malicious content. A recent example of this is the injection of anti-war messages in Russian TV programs [51]. Cabrera [36] showed an attack scenario using drones to replace the legit broadcast signal with crafted streams. In 2019, Massimo Bozza showed the feasibility and extreme easiness of hijacking HbbTV DVB connections through the use of the HiDes UT-100c, a modulator (transmitter)[13] and the C++ library TSDuck [24]. This weakness in the DVB architecture allows an attacker to perform a Monkey-in-the-Middle (MITM) attack replacing the original content of the HbbTV application with arbitrary and/or malicious content, such as fake news banners to spread misinformation, redirections to a malware-download website, or scam/phishing sites [35]. Similarly, Michéle et al. performed such an attack using a Terratec TStick+ as modulator and, on the software side, different libraries such as *tzap* [60]. Users might be tricked into clicking a malicious link, and JavaScript code can be run without the user's knowledge. For example, attackers can exploit TVs' CPUs to mine cryptocurrency using JavaScript-based code [74], [38], [54].

Ghiglieri and Waidner [47] conducted three different tests in 2012, 2014, and 2015 to analyze the HbbTV data flow from the Smart TVs to the broadcasters and vice versa, finding several privacy issues. A German channel transferred a user's login without HTTPS, thus allowing potential attackers to record the complete login process and later exploit it. In 2015, many channels switched to HTTPS for securing HbbTV applications indicating that some steps towards security and privacy maturity were being made. Despite this progress, no governing rules were still present, and such technology did not completely enforce users' privacy [60]. We revisit and extend this study to assess the current state of HbbTV across Europe.

**Anti-Tracking and Security Solutions.** Varmarken et al. assessed the (in)effectiveness of existing Smart TV DNS denylists showing that they do not successfully block all tracking [85]. Ghiglieri et al. proposed the Privacy Protector that allows users to control their data by barring channels from loading Internet data unless the user presses the *Green Button* on the TV's remote [45]. Mandalari et al. proposed a solution for generic IoT devices that could also be used for Smart TVs. Their idea is to flag domains as either "essential" or "non-essential" for the correct functioning of the device and block the latter [58]. Matejka et al. proposed a Security Manager [59] to ensure a secure authentication and authorization mechanism for users. Such an approach should verify that users are who they claim to be and later enforce some access control policies.

**Users' Risk Awareness.** A survey by Ghiglieri et al. [46] in Germany revealed that only a small percentage of respondents know of privacy and security risks, and even fewer can mention a concrete consequence. At the same time, when confronted with the risks, almost no one is willing to fully disconnect their device from the Internet. Malkin et al. conducted a similar survey on the risks of Smart TVs in the U.S., showing that participants are confused about what data are collected and how and by whom they are analyzed [57]. Nevertheless, respondents considered it unacceptable that their data is being repurposed and expected manufacturers to protect their data.

## IV. HBBTV PROTOCOL TESTING

To shed light onto current privacy issues introduced with the ongoing deployment of HbbTV in Europe, we start by describing our testing environment that allows us to intercept and analyze the content delivered by any TV channels supporting HbbTV. We present the issues we uncovered when studying 36 TV channels in Italy, Germany, France, Austria, and Finland using this environment in Section V.

**Methodology.** Our testing environment has two main components, as shown in Figure 2:

- *On-TV HTTP(S) Traffic Capture:* Listen and capture the traffic between the Smart TV and the servers to later analyze what domains are contacted and search for cookies and users' data (see Subsection IV-A).
- *Off-TV HTTPS Traffic Inspection:* Extract the URLs contacted by the Smart TV to launch the HbbTV app [35] and open them in a Chrome browser while a transparent proxy listens (see Subsection IV-B).

**Environment.** We use three main devices for our experiments: a Sharp Aquos LC-32Bi6, a Xiaomi Mi 4A Smart TV (Android 9), and a Samsung M5500 Smart TV (Tizen 3.0). In addition, we connect a laptop running Ubuntu 20.04 and Wireshark [26] through the Ethernet interface with the home router, and we enable its WiFi hotspot. We then connect the Smart TV to the WiFi network of the laptop.

Technically one Smart TV should suffice. However, two channels (see Subsection V-A; i.e., Mediaset and La7) did not receive any HbbTV application on the Android device, probably because of compatibility issues. Thus, we analyzed these channels on a Samsung device (where the HbbTV application is available and usable). Note that our off-TV testing approach does not require access to a Smart TV at all—as long as the targeted HbbTV URLs are known.

### A. On-TV HTTP(S) Traffic Capture

We record traffic for one hour in four phases (timings are the same adopted by Ghiglieri [45] to foster comparability):

1) Listen for 15 minutes without any interaction to spot information transmitted before user consent or explicit user action to enable the HbbTV application.
2) Give consent and interact for 20 minutes with the suggested buttons, different for each channel, to see what data is sent and if we spot HTTP connections in the extra features offered by the HbbTV application.
3) Revoke user consent (if possible) and listen for 10 minutes without interaction.
4) Restore consent, change the channel, re-tune back and listen for 15 minutes without any interaction.

We perform a factory reset of the TV for each channel analysis to prevent interference in the captured traffic.

We automate traffic analysis, for the Android device, with a bash script to precisely time the aforementioned phases. We collect traffic in *.pcap* files. To make the analysis process faster and more efficient, using Tshark [25], the command line version of Wireshark, we convert the *.pcap* file into a *.csv* file and extract the following information for HTTP(S) packets: *domain* (the contacted host), *occurrences* (the number of requests to a specific host), and *consent_status* (tags identifying the four periods the testing phase has been divided into).

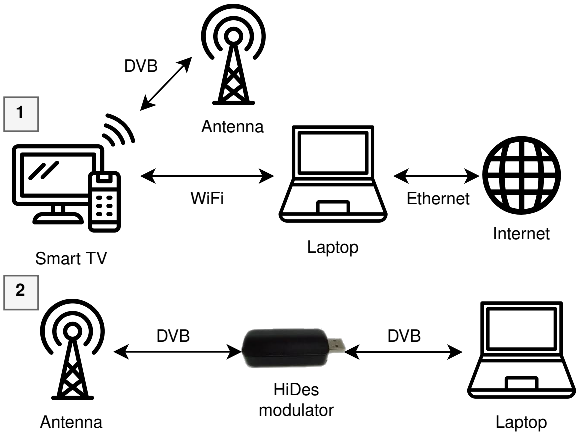

Fig. 2. Overview of our Testing Environment: (1) *On-TV HTTP(S) Traffic Capture* and (2) *Off-TV HTTPS Traffic Inspection*.

Additionally, we manually label each contacted service based on its intent and common usage (e.g., *Tracking*) by using publicly available online sources for each domain, e.g., we search for the organization owning the domain and analyze the main solutions offered by it. We exclude from our labeling domains that are contacted by the Smart TV itself and not because of the HbbTV application. Thus, we remove domains that are present in more than half of the traffic captures and that include the Smart TV vendor in the domain name, e.g., data.mistat.intl.xiaomi.com. Additionally, for unencrypted packets, i.e., using HTTP, we inspect them, looking for cookies, parameters, and API calls.

All the domains that we labeled as *Tracking* can signal misbehavior of the provider, i.e., not waiting for explicit user's consent before delivering tracking and targeted content—depending on whether we observed it either before the consent is given or after it is revoked. At the same time, even the non-tracking domains found before accepting the privacy notice are not in line with the HbbTV protocol, as no communication should occur unless the user agrees.

Furthermore, we analyze the timing between the requests to show whether there is a particular frequency of requests by computing the average time between requests to the same domain. The standard deviation shows if such a pattern is reliable (i.e., a high standard deviation means that the time window between requests varies significantly; therefore, we cannot identify a specific pattern).

### B. Off-TV HTTPS Traffic Inspection

For the second test, we start by extracting the HbbTV URLs from the DVB stream using the TSDuck library and the UT-100c HiDes modulator. As mentioned in Section II, the DVB stream includes the URLs of the HbbTV applications; thus, by analyzing the broadcast stream, we can extract them directly.

To do so, we perform a complete scan of the Ultra High Frequency (UHF) channels to identify the frequency of the channels to analyze using the `tsscan` function of TSDuck. Then, with `tsp`, we can capture the DVB stream on a specific frequency passing through the HiDes modulator in Transport Stream (TS) format. We then convert the file into a *.txt* format, and we extract the segments related to the Application Information Table (AIT), which contains the HbbTV information together with the start-up URLs of the applications, by specifying their respective Program IDs (PIDs). The `application_type` parameter should equal to `0x0010` meaning that the information is related to HbbTV.

We then open the extracted URLs in a Chrome desktop browser (version 91.0.4459.2), deleting the browser's data and cookies before each test to reset it, and following two approaches to mimic the Smart TV environment since some of the analyzed links can be opened only in one of the settings:

- *Browser Extension:* We emulate a Smart TV's browser with a Chrome extension (RedOrbit HbbTV Emulator [20]) that recognizes and renders `application/vnd.hbbtv.xhtml+xml` content.
- *Spoofed User Agent:* We change the User-Agent (UA) to one of a real Smart TV, e.g., `HbbTV/1.4.1 (+DRM+MEDIA360;Samsung;Smart TV2017; T-KTSDEUC-1290.3;;)+TVPLUS+ Smart HubLink Chrome`.

To collect traffic, we set up a transparent proxy using mitmproxy [15] on the same machine where we opened the extracted links to also intercept HTTPS traffic and capture its plaintext. We later manually inspect these files for analysis using the mitmdump component of mitmproxy. We perform this second test to bypass the limitations we faced when analyzing encrypted traffic in Subsection IV-A. One would expect the collected traffic to be very similar in the two test setups. However, since this latter approach might alter the communication between the Smart TV and content providers, we deem the first test necessary for completeness. In addition, the domains contacted with this second test, are for sure generated by interacting with the HbbTV application; thus, we can better filter out domains contained in the *On-TV* test that are not related to HbbTV but contacted by the Smart TV itself. Furthermore, this second setup provides better scalability and reproducibility, allowing anyone without access to a Smart TV to test selected HbbTV applications.

The methodology resembles our approach in Subsection IV-A, but we capture only 30 minutes of traffic: listen for 10 minutes without interaction, accept the privacy notice and interact for 10 minutes, revoke consent, and listen for 10 minutes. We extract the contacted domains and IPs with the known purpose of the service and tracking cookies.

## V. HbbTV Protocol Issues in the Wild

### A. Selection of TV Channels

Table I summarizes the selected channels, whether they are public or private, and their national audience share (if available). We performed a first round of tests between February and May 2021 from European countries where the selected channels are available. We conducted a second round of tests on November 2022 and marked the new channels accordingly. In 2022, we executed the *On-TV* test for 30 minutes more to spot potentially missed trackers (1h30 in total). As reported in Table I, for some channels, we performed the *Off-TV* test only for 10 minutes (5 without consent to the data policy, 5 with interaction) allowing us to respect our time constraints while fostering reproducibility and scalability.

TABLE I. Selected TV channels, their target country, whether the broadcaster is public or private, and their audience share [6], [5], [30], [78], [84], [21], [81], [79], [83]; ● signifies we both performed *On-TV* and *Off-TV* traffic inspection, ◐ means only the former and ◑ only the latter. In addition, we mark the channels we only tested in 2022 with *.

| | Country | Private/Public | Audience Share | Tests |
|---|---|---|---|---|
| **Rai1** | IT | Public | 11,54% | ● |
| **RDS** | IT | Private | - | ● |
| **RealTime** | IT | Private | 1.31% | ● |
| **SportItalia** | IT | Private | 0.22% | ● |
| **RTL** | IT | Private | 0,17% | ● |
| **Spike** | IT | Private | - | ● |
| **Canale 5** | IT | Private | 15,96% | ● |
| **La7** | IT | Private | 3,11% | ● |
| **Radio Kiss Kiss** | IT | Private | - | ● |
| **Radio Libertà*** | IT | Private | - | ● |
| **BOM Channel*** | IT | Private | - | ● |
| **NOVE*** | IT | Private | 1.92% | ● |
| **Caccia e Pesca*** | IT | Private | - | ◑ |
| **QVC*** | IT | Private | - | ◑ |
| **TeleNordEst*** | IT | Private | - | ◑ |
| **TeleChiara*** | IT | Private | - | ◑ |
| **SuperTennis*** | IT | Private | 0.25% | ◑ |
| **LineaGem*** | IT | Private | - | ◑ |
| **Warner TV*** | IT | Private | - | ◑ |
| **TV 8*** | IT | Private | 2.36% | ◑ |
| **HSE** | DE | Private | - | ◐ |
| **SWR BW** | DE | Public | - | ◐ |
| **Arte** | DE | Public | 1.3% | ◐ |
| **ZDF** | DE | Public | 14.2% | ◐ |
| **Anixe** | DE | Private | - | ◐ |
| **RTL*** | DE | Private | 7.3% | ◐ |
| **Das Erste*** | DE | Public | 11.9% | ◐ |
| **Sport1*** | DE | Private | 0.6% | ◐ |
| **Arte** | FR | Public | 1.3% | ◐ |
| **NRJ12** | FR | Private | 1.2% | ◐ |
| **ATV*** | AT | Private | 3.3% | ● |
| **ORF1*** | AT | Public | 8.4% | ● |
| **Servus TV*** | AT | Private | 4.7% | ● |
| **SchauTV*** | AT | Private | - | ● |
| **MTV3*** | FI | Private | 17.7% | ◐ |
| **Yle TV1*** | FI | Public | 27% | ◐ |

The Italian channels we selected belong to different broadcasters, either public or private. We chose these based on average audience share, broadcaster, offered content, and, of course, enabled support for HbbTV. For further comparison, we replicated the traffic analysis in Germany, France, Austria and Finland to reveal differences or similarities in adoption of the HbbTV protocol. For these, the procedure is similar but simpler. We carried out only the *On-TV* test (see Subsection IV-A), and we analyzed 30 and 90 minutes of traffic, in 2021 and 2022 respectively. For Germany, five of the total eight channels are a subset of the ones studied by Ghiglieri and Tews [45]: Arte, Anixe, SWR BW, HSE Live, and ZDF. Ghiglieri and Tews divided the channels they analyzed into four groups based on privacy invasiveness. For our study, we selected one representative channel from each group to see how the situation changed over five years. We selected HSE (a shopping channel) considering the gravity of security issues researchers found, e.g., handling credit card details over plain HTTP. In France, Austria, and Finland, the adoption of HbbTV is not yet in full swing, and few channels can interact with such applications. We report the channels we considered in Table I.

### *B. Privacy Related Findings*

**Italy.** We report the extracted HbbTV start links for the Italian TV channels we use for the in-depth test, including HTTPS interception, in Table VIII in Appendix D. Both tests (*On-TV* and *Off-TV*) aim to show what information is exchanged between the Smart TV and the broadcasters to investigate potential privacy risks. We thus aggregate and then present them in the following section.

Fifteen out of 20 Italian channels show connections to at least one tracking service (with possible profiling cookies) even before the user has a chance to decide whether or not to accept the privacy notice. Table II summarizes which channels connect to which tracking service before users' consent, including different Google tracking and analytics services. In addition, three channels make POST requests to an Amazon Web Services (AWS) API /audiencesavemessage with the user ID, model, and device brand as parameters for profiling.

In general, cookies have long expiration dates ranging from the year 2021 to 2048. Such cookies can track users' behavior with potential linkage to other data; therefore, such persistence poses privacy risks. The situation seems to have improved in 2022, as the longest expiration date we found is December 2023. Additionally, given the adoption of HTTP by some services, such cookies are sent in plaintext. If an attacker is sniffing the communication channel over which the information is sent, they can intercept it. For example, RealTime sends plaintext cookies identifying the user's geographical location and Internet Service Provider (ISP) and sets Google Analytics ones even before their explicit consent.

Six channels do not present any privacy policy when accessing the HbbTV application for the first time, and the user starts to be profiled without having provided consent. Such a policy is nowhere to be found even in the sub-menus of the app. On the other hand, since 2021, two channels, RDS and Rai, that did not show any policy, now prompt the user with a privacy banner showing some progress.

Some channels offer the possibility to revoke the consent given to data processing later, while others do not. Since deleting cookies on the Smart TV is not trivial (in fact, such a procedure typically requires a factory reset) and given the cookies' long expiration dates, it would be fair to provide the user with the possibility to revoke the consent to data processing. Specifically, ten channels out of the 20 we examined do not allow users to withdraw consent.

Moreover, despite presenting the possibility of revoking consent, the channel RTL, in reality, does not delete profiling and identification cookies, and requests to any tracking services are still made even *after the user revoked their consent*.

We further found that a widely used tracking technique by broadcasters is the *tracking pixel* [43], i.e., tracking user behavior by uploading a $1 \times 1$ pixel image when the user visits a website or opens a particular content. Given its small size, it is invisible to the naked eye. Still, it can provide valuable data to advertising or analytics companies that can infer user preferences in this way. In particular, seven channels adopt this technique by returning $1 \times 1$ pixel GIF89a objects in requests.

Finally, similar to the results reported by Ghiglieri et al. [47], some channels perform periodic requests to check if the user is still watching. What we noticed are periodic requests for tracking services. Almost all channels show frequent requests to profiling domains (on average, around every minute); for example, SportItalia makes requests to Smartclip (an advertisement broker in the Addressable TV ecosystem) around every 70 seconds, while RDS contacts Google Analytics around every 14 seconds. A low standard deviation indicates that we identified a recurrent pattern.

**Germany.** All five channels present privacy policies. However, just two of them, Arte and HSE, show the privacy policy as soon as the user opens the respective channel. In the other cases, we have to search for it in the sub-menu of the HbbTV app or click the blue button. All channels offer the user the possibility to revoke their consent. Still, SWR, Arte, and ZDF offer the user only the option to disable the tracking pixels.

All five channels adopt tracking pixels. In addition, in 2021, we observed more "in-house" tracking (using smaller and/or local companies), unlike the Italian channels that rely on larger services such as Google Analytics or Smartclip to collect user information. This phenomenon faded in 2022 as we noticed the use of larger services also by the German channels. By nature, larger third-party services, such as Google, have the means to aggregate more user data, e.g., with information collected from websites and mobile apps. This opens the potential for more targeted content and advertising, possibly across a user's devices (not limited to the Smart TV).

We also found greater use of HTTP, i.e., unencrypted traffic, than we observed in Italy. This leads to serious security issues: two channels, Arte and HSE, allow users to log in using their credentials linked to an account holding sensitive information, such as their address and credit card information. The credentials are sent in plaintext, allowing an attacker to intercept them. This issue was already explicitly reported in a previous paper for HSE in 2014, but is still not fixed [45].

Overall, we observe that the security and privacy posture of German TV channels, unfortunately, has not evolved much from what Ghiglieri et al. already observed in 2015.

**France.** On a positive note, both channels show the privacy policy before interacting with the app and allow the withdrawal of consent. Conversely, as in Germany, Arte supports the aforementioned tracking pixel. We also observe greater use of smaller/local tracking companies. As in Germany, Arte offers the possibility of logging in, but sends the authentication code in plaintext, thus allowing attackers to intercept it.

**Austria.** All four channels adopt the tracking pixel; In particular, track.tvping.com, which returns a $1 \times 1$ pixel PNG, is contacted by all of them with a request *every second* even before consent is given. Despite all the channels presenting the privacy policy, this is shown only once the user starts interacting with the HbbTV application. Finally, although Servus TV presents the option to revoke cookies, this functionality is not correctly implemented, and tracking cookies are always on.

**Finland.** For Finland, we observed the absence of a privacy policy and the option to revoke consent for the MTV3 channel. In addition, both channels uniquely rely on HTTPS for communication and do not adopt the tracking pixel.

TABLE II. Summary of our Results: We report (1) which tracking service the channels contacted before users' consent, (2) whether we could locate a privacy notice, (3) if revoking consent was possible, (4) if a tracking pixel was used, (5) whether channels performed periodic requests to tracking domains and (6) whether the channel uses plain HTTP. ● = "Yes", ○ = "No", ◐ = "Partially". The latter applies when we could only partially revoke consent (e.g., disable tracking pixels but not revoke consent to the rest of tracking). We mark the channels we only tested in 2022 with a *.

| | Channel Name | Tracking Services | Privacy Policy | Revoke Consent | Tracking Pixel | Periodic Requests | HTTP |
|---|---|---|---|---|---|---|---|
| **ITALY** | **SportItalia** | DoubleClick<br>POST to /audiencesavemessage (AWS)<br>ip-api | ● | ● | ○ | ● | ● |
| | **RDS** | - | ● | ◐ | ○ | ○ | ○ |
| | **RealTime** | Google Analytics<br>Google Tag Services<br>discovery-log-view.castoola.tv<br>atv-discovery-microservices.castoola.tv | ● | ○ | ● | ● | ● |
| | **RTL** | - | ● | ◐ | ○ | ● | ○ |
| | **Rai 1** | Scorecard Research | ● | ◐ | ● | ● | ○ |
| | **Spike** | Google Tag Services<br>SecurePubAds | ● | ● | ● | ○ | ● |
| | **Canale 5** | tags.tiqcdn.com (Tealium Inc.) | ● | ● | ○ | ● | ● |
| | **La7** | tags.tiqcdn.com (Tealium Inc.)<br>DoubleClick<br>cdn.permutive.app<br>smetrics.rcsmetrics.it | ● | ◐ | ● | ● | ○ |
| | **Radio Kiss Kiss** | POST to /audiencesavemessage (AWS) | ● | ○ | ○ | ● | ● |
| | **BOM Channel*** | - | ○ | ○ | ○ | ○ | ● |
| | **Radio Libertà*** | analytics.persidera.it | ○ | ○ | ○ | ○ | ○ |
| | **NOVE*** | Google Analytics<br>Google Tag Services | ● | ○ | ● | ● | ● |
| | **Caccia e Pesca*** | tags.tiqcdn.com (Tealium Inc.)<br>smetrics.rcsmetrics.it<br>components2.rcsobjects.it/rcs_tracking-service | ○ | ○ | ● | ○ | ○ |
| | **QVC*** | INFOnline GmbH | ● | ● | ● | ● | ● |
| | **TeleNordEst*** | - | ● | ○ | ○ | ○ | ○ |
| | **TeleChiara*** | DoubleClick | ○ | ○ | ○ | ○ | ● |
| | **SuperTennis*** | analytics.persidera.it | ○ | ○ | ○ | ● | ○ |
| | **LineaGem*** | DoubleClick<br>POST to /audiencesavemessage (AWS)<br>ip-api | ● | ● | ○ | ● | ● |
| | **Warner TV*** | - | ● | ◐ | ○ | ● | ● |
| | **TV 8*** | DoubleClick<br>Google Tag Services | ○ | ○ | ○ | ○ | ○ |
| **GERMANY** | **HSE** | hse24.tvtelemetrie.de | ● | ● | ● | ○ | ● |
| | **SWR BW** | - | ● | ◐ | ● | ● | ● |
| | **Arte** | XiTi by AT Internet | ● | ◐ | ● | ○ | ● |
| | **ZDF** | XiTi by AT Internet | ● | ◐ | ● | ● | ● |
| | **Anixe** | Google Analytics | ● | ● | ● | ● | ● |
| | **Das Erste*** | - | ● | ● | ● | ● | ● |
| | **RTL*** | tvping.com<br>Smartclip<br>nmrodam.com by Nielsen | ● | ● | ● | ● | ● |
| | **Sport1*** | Smartclip<br>tvping.com | ● | ● | ● | ● | ● |
| **FRANCE** | **Arte** | XiTi by AT Internet<br>Médiamétrie | ● | ● | ● | ● | ● |
| | **NTJ12** | DoubleClick<br>mediarithmics<br>XiTi by AT Internet | ● | ○ | ○ | ● | ○ |
| **AUSTRIA** | **ATV*** | tvping.com | ● | ◐ | ● | ● | ● |
| | **ORF1*** | tvping.com | ● | ◐ | ● | ● | ● |
| | **Servus TV*** | Google Tag Services<br>tvping.com | ● | ○ | ● | ● | ● |
| | **SchauTV*** | Smartclip<br>tvping.com | ● | ● | ● | ● | ● |
| **FINLAND** | **MTV3** | - | ○ | ○ | ○ | ○ | ○ |
| | **Yle TV1** | - | ● | ◐ | ○ | ● | ○ |

TABLE III. THE FRACTION OF TRACKING DOMAINS WE FOUND IN OUR HBBTV ANALYSIS (70 IN 2021 AND 43 IN 2022) INCLUDED IN WIDELY USED TRACKING DENYLISTS. WE LOOK AT PI-HOLE [17] (VERSION OF MAY 23, 2022) AND EASYLIST [9], A POPULAR SET OF RULES FOR ADBLOCK (VERSION OF MAY 23, 2022, AND MARCH/APRIL 2021).

| | Configuration | Total Rules /Domains | 2021 Blocked (out of 70) | 2022 Blocked (out of 43) |
|---|---|---|---|---|
| Pi-hole | Default [23] | 115,065 | 31 (44.29%) | 35 (81.39%) |
| | SmartTV [3] | 167 | 1 (1.43%) | 2 (4.65%) |
| | Samsung SmartTV [1] | 73 | 0 (0%) | 0 (0%) |
| | SmartTV2 [2] | 213 | 2 (2.86%) | 6 (13.95%) |
| EasyList | March/April 2021 | 57,276 | 5 (7.14%) | 4 (9.30%) |
| | Privacy – March/April 2021 | 22,136 | 3 (4.29%) | 3 (6.98%) |
| | May 2022 | 60,680 | 11 (15.71%) | 5 (11.63%) |
| | Privacy – May 2022 | 26,939 | 7 (10.0%) | 6 (13.95%) |

### C. Identified Trackers

During our analysis, we identified (i.e., manually attributed) 70 domains to advertisement and tracking services in 2021, as well as 43 in 2022 (19 domains are shared between both years). In Table III, we report the numbers of tracking domains we found during our analysis and whether they are contained in (and thus could be blocked by) currently available denylists. Similar to related work on web tracking, our results show limited coverage of these lists [43]: in the best case, 31 out of 70 (44.29%) of the tracking domains are known and thus can be blocked. This "best-case scenario" is Pi-hole [17], a network-level ad and tracker blocking application based on DNS sinkholes. It is designed to block general web trackers, mobile app trackers, as well as trackers part of the firmware and applications installed on certain Smart TV models.

When comparing the results between March/April 2021 (when we performed our network captures) and the most current EasyList as of May 2022, we see a small uptick in the included domains (5 to 11, and 3 to 7 in the general and Privacy version, respectively). This indicates that filter lists are catching up to new players in the Smart TV advertisement ecosystem, but the overall coverage still remains low.

## VI. USERS' RISK AWARENESS

Our findings presented in Section V on a sample of 36 TV channels highlighted how broadcasters do not always protect users' privacy. However, the adoption of the HbbTV protocol by broadcasters, as well as the integration of new, and more privacy-invasive, features (such as targeted ads via Addressable TV) is still ongoing. To understand whether European users' are aware of the risks associated with this new TV viewing experience, we conducted an anonymous survey on a sample of 174 individuals in Italy. We reached the sample by spreading the URL of the online survey over social media platforms (e.g., Facebook groups), trying not to introduce bias in the selection, i.e., targeting groups without a specific background or interest. However, this cannot be ruled out. The only requirements to participate in our survey was that participants are older than 18. The language of the survey was Italian.

Our survey expands a survey conducted by Ghiglieri et al. [46] that assessed the level of users' awareness concerning privacy and security with HbbTV in 2015. Ghiglieri et al. conducted their questionnaire in Germany. As reported in Section III, it confirmed a generally low level of awareness of privacy- and security-related risks in this context. It also showed that, even if exposed to the risks from the uncontrolled use of Smart TVs, users are not willing to fully disconnect their devices from the Internet to avoid losing the extra features offered. Thus, a solution that provides security (against ill-intentioned attackers), privacy, and functionality is needed.

**Methodology.** We generally follow the approach adopted by Ghiglieri et al. [46], with the following differences: (1) We perform our survey six years after theirs (i.e., "post-GDPR"), (2) in a different country (Italy instead of Germany), and, most importantly, (3) with more targeted questions that focus on HbbTV rather than general Smart TV security. Our goal is to see whether users' awareness has improved with the more widespread adoption of HbbTV and Smart TVs, and whether Italian users have a different approach to privacy than German ones. We adopt a mixed-method design by including quantitative and qualitative methodologies. We include both closed questions (multiple- or single-choice) and semi-structured open-ended ones. We analyze the latter by adopting an open coding approach; we cluster answers into categories and assign them a code to perform additional analysis later. We present the initial codebook in Table VI in Appendix B. We built the study using SoSci Survey, a German platform that allows for heavy customization of sections [22]. Their servers are located and operated in Germany and data are processed according to GDPR specifications.

**Ethical Considerations.** When conducting the survey, we fully respected the ethical guidelines defined by the University of Twente, and we received approval from its ethical committee.

In addition, on the first page of the questionnaire, we report our contact information for the participants and explicitly state that participation is voluntary; respondents can stop the survey at any point, and we do not consider the answers they give if they decide to do so. Furthermore, we inform participants that we use the gathered data only in the context of this study.

We put particular care into anonymizing the results; although we do not ask for Personal Identifiable Information (PII), participants might disclose such information in the open questions. When defining the codebook, we exclude any PII.

**Survey Structure.** Due to space constraints we only provide a summary of our survey structure, but provide the full survey briefing and questions online for the interested reader [10].

1) *Introduction*: we inform participants about the topic of the survey. We omit some technical details not to influence their answers. We include survey details, such as its anonymity and the duration.
2) *(Smart) TV Demographics*: we ask participants whether they own a TV or a Smart TV. We ask those who do not own a Smart TV if they would consider buying one. Only those who own a Smart TV, or want to buy one, continue to the next section. We redirect the others to "Final Questions."
3) *Awareness of Security and Privacy Risks*: we ask participants if they are aware of security and privacy risks of Smart TVs; if yes, they should enumerate them and eventual measures to counteract these risks.

4) *HbbTV Statistics*: we ask participants whether they ever encountered HbbTV notifications and if they are aware of how such protocol works.
5) *Risk Assessment of Scenarios*: we give participants eight different risky scenarios for HbbTV (one per page) in random order. For each scenario, we ask them to give a score based on how critical they think it is. The score ranges from 1 (very low risk) to 5 (very high risk) similar to a Likert scale. Additionally, we ask participants to justify their rating. We provide the full list of scenarios in Appendix A.
6) *Privacy Policy Questions*: we ask participants whether they read privacy policies when accessing digital services and if they were ever shown banners asking for data treatment consent when watching TV.
7) *Selection Grid*: we present participants with a table showing five modalities, reported in Appendix C, of connecting the TV to the Internet with different security levels and extra functionalities available. We ask them to vote for their preferred one and also mention all the desired features that a tool to enforce security in this context should have.
8) *Final Questions*: we ask participants their age, gender, and their area of expertise to have insights on the demographics of our participants.

**General Statistics.** 817 people received the URL pointing to the survey. 174 participants completed it, with 55 providing female (32%), 116 male (67%), and 3 (1%) other as gender. The youngest participant was 18, the oldest 80, with a mean age of 37.6 years and a standard deviation of 14.8. Out of the 174 participants, 132 answered that they either possess a Smart TV or would be willing to buy one. Those continued the study while we redirected the others to the Final Questions section. In the remainder of this section we only consider the 132 responses and omit the remaining 42 ones.

**Security and Privacy Awareness.** 90 participants (68%) did not mention any risk—confirming an alarmingly low level of awareness, although showing a significant improvement from the 2015 survey where 84% of the participants did not report any risk; 26 (20%) participants identified only one risk; the remaining (12%) identified either 2, 3, or 4 risks. The most frequently mentioned risk relates to privacy and consists of tracking and profiling (26 participants, 20%). The second most frequent answer (17 participants, 13%) is data and credential leakage due to unencrypted traffic or unreliable services. Lastly, only 26 participants (20%) mentioned at least one security measure to prevent such risks, with firewalls the most cited answer (9 participants, 7%).

**HbbTV Statistics.** 77 participants (58%) reported having seen HbbTV notifications while using their Smart TVs, showing an increased user percentage from the 2015 survey. However, only 15 (11%) correctly mentioned that such protocol is a combination of standard broadcast signal and broadband communication to deliver Internet-based content.

**Risky Scenarios.** When presented with broadcasters being able to store and analyze usage habits (scenario 4), participants assigned an average risk value of 2.88. All it took was adding that the information is used to show personalized advertising (scenario 2), to raise this value to 3.09. In addition, respondents gave a risk score of 3.49 to broadcasters who might aggregate data from other services and sell information to third parties (scenario 8). This highlights how users are concerned about how their data is used for profiling, but there is little awareness. The responsibility and duty are then in the hands of broadcasters to ensure the consensual handling and collection of their users' data. For the complete risk scoring assigned to each scenario, refer to Table IV. Finally, we compare values assigned to the first four scenarios in the 2015 survey. We notice a slight decrease in participants' risk scores. Still, values are comparable, and security seems to be a major concern.

TABLE IV. Mean risk scores assigned to the eight scenarios and their standard deviation ($\sigma$) compared to Ghiglieri et al.'s survey [46] from 1 (very low risk) to 5 (very high risk).

| Scenario | IT (2022) | DE (2015) [46] |
|---|---|---|
| 1: Aggregation of usage data (viewing habits) | 2.70 ($\sigma$=1.04) | 2.82 (–) |
| 2: Collection of usage data for personalized ads | 3.09 ($\sigma$=1.09) | 3.16 ($\sigma$=1.41) |
| 3: Collection of usage data for unclear purpose | 3.42 ($\sigma$=1.13) | 3.64 ($\sigma$=1.28) |
| 4: Collection of usage data for TV broadcasters | 2.88 ($\sigma$=1.12) | 3.22 ($\sigma$=1.44) |
| 5: Shopping personalized ads | 3.63 ($\sigma$=1.19) | N/A |
| 6: Shopping personalized ads with insecure handling | 3.97 ($\sigma$=1.15) | N/A |
| 7: Data aggregation for personalized content | 3.05 ($\sigma$=1.06) | N/A |
| 8: Data aggregation for personalized ads | 3.49 ($\sigma$=1.05) | N/A |

Compared to a study by Malkin et al. in 2016 in the U.S. [57], Italian participants seem to be more concerned about personalized content. Out of the 591 respondents in the U.S., most found acceptable that viewing history is shared with broadcasters to improve personalized suggestions (as long as such information is not repurposed). Furthermore, when asked if they thought data could be repurposed (e.g., for ads), only 37% of the U.S. participants listed this as a possible scenario.

**Privacy Policies.** Of our 132 participants, 90 (68%) stated that they never or rarely read the privacy policy presented when accessing a digital service for the first time, and 123 (93%) indicated that they did not read such privacy policy presented while watching a TV channel (or were not able to answer). Only 47 respondents (35%) mentioned at least one type of data that could potentially be collected while using an Internet-connected Smart TV. The most mentioned collected type of data is "viewing times and preferences" (36 times), while the second most is "personal information," e.g., email addresses and birth date (10 times). Only 4 (3%) participants mentioned that broadcasters could collect their geographical location.

**Preferred Usage of Smart TVs.** Lastly, we asked participants how they would like to connect their Smart TV to the Internet, considering security aspects, functionality, required effort, and costs. 45 participants (34%) preferred the cheaper solution that requires some configuration to secure the Internet communication of the Smart TV. Only 23 participants (17%) voted for connecting the device without further security measures, while 80 respondents (61%) would be willing to adopt some solution to improve security. The most mentioned features to consider when designing a tool to protect Smart TVs are "ease of use" (28 times) and "highly customizable" (25 times), with eventually two different options for both expert and non-expert users. Conversely, Malkin et al. showed their participants would likely be willing to give up (at least theoretically) some extra features to prevent data sharing [57].

## VII. HbbTV Blocker

To mitigate the privacy issues described in Subsection II-B and Section V and to protect users against broadcasters that are not privacy-compliant and/or misconfigured, we designed and developed a prototype for an HbbTV Blocker. HbbTV Blocker demonstrates how a simple yet effective denylist-approach similar to adblockers in the web and mobile domain can be deployed in this domain. Our implementation consists of a gateway that intercepts traffic to and from the Smart TV and domain filter lists on a per-TV-channel basis. We present the architecture of the HbbTV Blocker in Figure 3

**Gateway vs. Proxy.** In our proof-of-concept deployment, we use a Raspberry Pi [19] as the gateway and connect it via Ethernet to Internet router while we connect the Smart TV to the WiFi hotspot of the gateway. In such a way, all the traffic directed to the Smart TV passes through the gateway. We designed the prototype to work on nine Italian channels studied in Section V. Expanding the tool to other channels is straightforward but would require us some manual effort. We plan to automate this procedure further to extract HbbTV URLs and ease the inclusion of new TV channels.

The reason why we chose a gateway over the proxy used by Ghiglieri and Tews in their Privacy Protector [45] is twofold. On one side, they adopted mitmproxy as a transparent proxy which requires its CA to be installed in the Smart TV to capture HTTPS traffic. Root access is required to install such certificates. Unfortunately, gaining root privileges on a Smart TV is not easy since no documentation is available, and every different model has its custom procedure (if any). Their approach worked fine a few years ago when primarily only HTTP was used in HbbTV communication, but it requires more effort with the increased adoption of HTTPS.

Additionally, even with simpler proxies that do not act as MITMs but collect traffic headers, there is a problem when setting those on Smart TVs. Android proxy settings apply only to browser traffic. Other applications' traffic, including HbbTV, even though technically it is also rendered in a browser, does not pass through the proxy for security reasons. Root access is required to bypass this limitation [63]. Thus, we deemed the gateway approach the best in terms of universality and adaptability to different models, brands, and operating systems of Smart TVs considering the requirement of "ease of use."

**Channel Identification.** As a first step, HbbTV Blocker identifies the TV channel a user is currently watching. To do so, a Python script intercepts DNS queries using the pyshark library [18] (a wrapper for tshark), and filters them. If the contacted domain matches against specific string patterns defined for each of the nine channels (see Table VIII in Appendix D), we set the current channel to the matched channel.

**Per-Channel Denylist.** We create a denylist of domains for each channel based on the tracking and analytics domains identified in Section V. To enforce those lists, we use *iptables* [14]. For each entry in the denylist, we add a new rule to block this specific traffic. The format of the rule is the following `iptables -A INPUT -m string --string "domain" --algo bm --to 65535 -j DROP` with *domain* being replaced with the current entry.

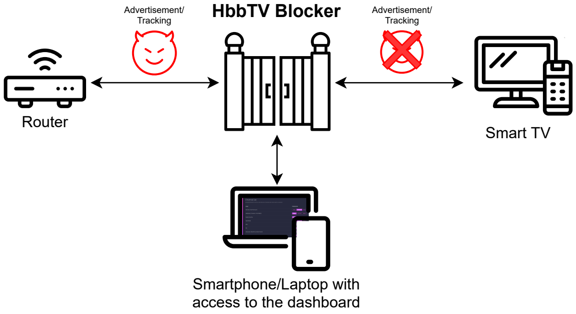

Fig. 3. Overview of HbbTV Blocker in our testing environment.

We preferred the approach of denylists over allowlists: The latter would require defining a specific set of allowed domains for each application used by the user. Thus, we would risk unintentionally blocking this traffic whenever a user installs or uses a new application on their Smart TV. Additionally, defining allowlists for services like Google or Amazon AWS is a non-trivial task considering the number of domains and subdomains they use. Thus, we deem the denylist approach more scalable if new applications are installed and easier to manage. Other widely used tools, for example, Pi-hole [17], also adopt this solution to block unwanted traffic but do not offer the same granularity as HbbTV Blocker.

For each channel, we individually test the domains we flagged as tracking to evaluate if blocking them causes some breakage of the HbbTV application's intended functionalities. If by blocking such the application stops working, we exclude them from the channel denylist as this would mean losing the extra interactions offered by the broadcasters.

In addition, we decided to check for new tracking and advertisement domains by matching incoming traffic to the most recent versions of Pi-hole and EasyList lists. The users will then be displayed with the flagged domains and have the option to block them. We consider this necessary as such lists also block domains necessary for the correct functioning of the HbbTV application as hbbtv.mediaset.net.

**HTTP Blocking and Upgrade.** HbbTV Blocker additionally offers the option to block all HTTP traffic via the following iptables rule `iptables -I FORWARD 1 -p tcp --destination-port 80 -j DROP`. Although receiving only encrypted traffic might be a good security practice, blocking all HTTP traffic might hinder the HbbTV application's functionalities. A better solution would be upgrading all HTTP traffic to HTTPS (if the remote endpoint supports it, similar to Desktop browsers), which we leave for future work.

**Configuration.** We designed our approach with ease of use and customization in mind based on users' preferences expressed in our survey in Section VI. We provide the user with a graphical dashboard where different options are available; they can decide each channel's traffic behavior, block all HTTP traffic, get an overview of the number of blocked requests per channel, and upload customized denylists. In particular, the user can select three modes of operation:

- **Allow all**: all the traffic, including tracking and profiling, passes through the gateway.
- **Block tracking**: enforces the denylists designed to block tracking and analytics domains.
- **Block all**: blocks all traffic.

The *Block all* modality might hinder user experience since it also blocks traffic unrelated to HbbTV. We present the user with an informative alert when turning on this option.

We acknowledge that HbbTV blocker shifts the responsibility to the users of the Smart TV: they have to maintain the tracking denylists to ensure they are updated and complete. However, we provide the user with a trade-off between deciding to block all traffic and potentially impeding functionality or only selectively blocking certain domains. Again, we took Pi-hole as inspiration since most of its available denylists are written by the community of users and shared across them. Users can easily upload the updated denylist via the graphic interface they have access to.

**Usability Testing.** To verify that we respected the criteria of "ease of use" and "customization" highlighted by the user survey in Section VI we conducted an in-person moderated study on a sample of five participants. Each interview lasted for 20 minutes, and we asked participants to install and interact with our tool (we gave them a Raspberry Pi with Raspian already installed for time reasons and being its installation out of scope for our usability study). We informed our participants what data we were gathering and how we used it in the context of this study. Finally, we asked for their consent before and after the interview to respect ethical guidelines.

Participants generally did not report any difficulties in interacting with the HbbTV Blocker. Nevertheless, we received suggestions such as having a dedicated page for unexperienced users with a recommended configuration, i.e., that blocks tracking traffic without breaking functionalities. In addition, participants reported in some cases that options needed an adequate/simple description to understand them fully. We fixed the issues highlighted by our respondents.

**Performance Evaluation.** We used a Raspberry Pi 4 with 8GB of RAM and collected the number of packets exchanged per second and the number of bytes per second, CPU, and RAM usage. Such measures are collected by a script every 10 seconds to avoid the observer effect. As described above, we connect the Raspberry Pi through the Ethernet interface to the router and the Smart TV to its WiFi hotspot. Then for 30 minutes, we use the TV to navigate the channels and utilize their HbbTV applications. We report the results in Table V for when the Raspberry Pi is idle, i.e., HbbTV Blocker was not running, and when it was active. Despite increasing resource usage, our results indicate that the tool is not highly demanding. Additionally, the relatively low number of exchanged packets for HbbTV applications makes the tool suitable for its intended task of blocking requests without interruptions of the viewing experience.

In addition, we compute the latency introduced by our architecture. We run *curl* 100 times on three different HbbTV URLs (hbbtv.rds.radio, ht.la7.it/index.php, discovery.castoola.tv/realtime) with the Smart TV directly connected to the router or through the Raspberry Pi and extract the request time. We see an increased time in handling the requests; for the first URL, the average time in seconds is 0.012 and 0.28 without and with the Raspberry Pi, respectively. Nevertheless, a higher standard deviation in the second case (0.99) shows that a few requests took a long time, making the average not a trustworthy measure for latency. The median, instead, is 0.021 seconds, showing a reasonable overhead.

TABLE V. Performances Tests Results of HbbTV Blocker.

| | **Idle** | **Running** |
|---|---|---|
| **Average CPU usage (%)** | 3.70% | 35.66% |
| **Average RAM usage (%)** | 11.14% | 14.66% |
| **Average Packets per second** | 0 | 256 (max 7,433) |
| **Average KBytes per second** | 0 | 176 (max 7,600) |

**Comparison with Existing Tools.** Most of the solutions we discussed in Section III are dependent on TV manufacturers, i.e., they block tracking carried out by the latter. As we investigated, the denylists proposed are insufficient to protect users against the heavy tracking of HbbTV-enabled channels, although currently representing one of the best approaches to defend against privacy risks. Solutions, such as the Security Manager proposed by Matejka [59], only focus on the security and privacy of independent apps; instead, HbbTV runs as a web application in the TV's built-in browser. Thus, we deem HbbTV Blocker a necessary solution to protect users against the significant tracking carried out via the HbbTV protocol.

## VIII. Discussion

Both the results presented in Section VI and Section V highlight a problematic immaturity in the context of HbbTV adoption on both broadcasters' and users' sides. The results of our technical analysis show the negligent behavior of broadcasters offering HbbTV applications. Fair treatment of users' data is not always guaranteed, as we demonstrated with the connection to tracking services before their consent. Remarkably, we find several violations of GDPR. Tracking before the user has expressed their consent contradicts the "Conditions for consent" of the European Regulation and the guidelines on cookies by the Italian GPDP. Additionally, withdrawing consent, with the consequent deletion of data, should be possible and as easy as giving it according to the same statement of GDPR. We show this is not the case for channels that do not allow consent revocation or ask the user to contact their dedicated office directly. Even channels allowing consent revocation only do so partially, or in one case, not honor the users' consent revocation at all. The absence of the privacy notice when accessing the HbbTV application for the first time, as for TV8, signals a violation of transparent information communication and the provision of correct information to the data subject. As for ORF, the "hidden" policy in a sub-menu of the app violates the principles of transparency. The incorrectness, incompleteness, and non-transparency of the privacy policies presented by the different channels do not help users understand what information is collected and how it is processed. This violates the principles of processing personal data, the provision of the correct information, and transparency.

Users seem unaware of the potentially privacy-invasive appliance they have in their homes. This likely comes from a past mental model where TVs were just "secure" and their communication channel uni-directional, i.e., users were mere consumers of TV content. When we asked about the risks associated with Smart TVs or HbbTV, only few participants could mention at least one. Despite this lack of awareness, when confronted with potentially risky scenarios, users seem to be highly concerned about their data and personal information, e.g., viewing preferences, even more than what was reported by Ghiglieri in his survey on German users [46] in 2015. This highlights profound technical illiteracy, possibly leading to privacy problems for unaware users.

The consequences of having such a "relaxed" approach towards privacy in the Smart TV context, and more specifically towards the HbbTV protocol, could lead to several issues. In particular, additional issues arise from adopting dynamic and targeted advertising, now being pushed as part of "Addressable TV" by several players in this ecosystem [55], [4], [7]. With their persuasive power, algorithms can "nudge the behavior of data subjects and human decision-makers by filtering information" [61]. In the HbbTV context, users are encouraged to buy certain suitable products. Additionally, users' data can be aggregated and used for better profiling without their awareness. However, the risk does not necessarily stop there: we argue that while users have become more accustomed to targeted advertisement when surfing the web and using mobile apps, they are still used to the "linear TV" experience where the same content is provided to all viewers. Additionally, they might put particular trust into certain TV broadcasters, such as public and well-established news channels. However, with this paradigm shift, content, including (potentially political) advertisement can be highly personalized and targeted—by both private and public TV broadcasters and channels.

In terms of security risks, HbbTV content is not always encrypted, thus potentially leading to MITM attacks that can replace the HbbTV app's URL to load a different content or overlay it. This could be abused to spread misinformation through fake news, or for phishing attacks. Users can directly interact with interactive ads to make online purchases. As no sanitization or additional checks on the URL's source is performed, an ill-intentioned party could replace legit ads with malicious ones; thus, tricking the user into inserting sensitive data in a fake checkout page.

Finally, the advent of online shopping apps via HbbTV is already a reality in Germany and will not take long to reach other European countries. The user must insert sensitive data such as credit card information, billing address, and name to purchase online. The incorrect handling of this data might lead to severe security issues, such as theft of personal information and credentials. As reported in Section V, the use of plain HTTP with no encryption of data when logging in to such services poses a serious threat to the user. Even more worryingly, in the case of HSE, this issue has been known since 2014, but still persists. To protect users from misconfigurations on the broadcasters' side, browsers on Smart TV's should catch up with their desktop counterparts, which nowadays upgrade connections to HTTPS by default. To further protect connections from eavesdropping, certificate pinning could be an option, but comes with maintenance overhead and again the risk of misconfiguration [68].

### A. Key Takeaways

Following the discussion of the privacy implications of our findings, we highlight our main takeaways:

- All the 36 TV channels we analyzed contact at least one tracking domain; further, 26 communicate with trackers before the user has expressed their consent. Seven channels do not present any privacy policy when accessing them for the first time.
- 20 of the 36 TV channels (56%) we analyzed adopt the invisible "tracking pixel" to profile users.
- Commonly used tracking denylists only block at maximum 44% in 2021 and 81% in 2022 of the domains in our traffic captures and marked as tracking.
- We found HTTP communication in most of our traffic captures; such traffic contained sensitive information such as device IDs, visitor IDs, country codes, and ISP information.
- The shopping channel HSE allows users to create accounts and log in over plain HTTP, thus exposing sensitive information to potential attackers (e.g., credentials and credit card number).
- Out of the 132 participants in the Smart TV and HbbTV awareness survey, 68% could not mention any security or privacy risk, and 68% stated they never read privacy policies presented by digital services.
- When confronted with risky scenarios, respondents' average risk score (from 1, low, to 5, high) ranges from 2.70 to 3.97; thus, users are highly concerned with their security and privacy but unaware of the risks.

## IX. Limitations and Future Work

For our study of TV broadcasters' privacy posture, we only selected a subset of channels that offer HbbTV functionalities based on different parameters, e.g., audience share. To complement our study, we plan to include further channels to have a complete overview of the HbbTV landscape in Europe.

Our user survey relies on self-reporting; therefore, we cannot verify whether the participants' claims correspond to their actual behavior when interacting with a Smart TV. Several studies have highlighted this discrepancy between self-professed privacy attitudes and actual behavior [70], [69], [53]. The understanding of how attitudes and behaviors diverge represents an orthogonal research challenge.

We intend HbbTV Blocker as an initial step in its development, which should be considered a prototype. We do not consider the performance results reported in Section VII as complete, but they only glance at the resources' usage. We would further require usability testing to verify whether further customization options are needed and whether it fulfills the "ease of use" requirement. Furthermore, the *Block all* feature might impede a Smart TV's functionality; there is no straightforward way to detect when the user exits the "standard" TV channels and switches to a different app, such as YouTube, which might lead to unintended blocking. Still, we provide HbbTV Blocker's code as open source and argue it could be expanded with modules blocking tracking traffic on other smart home appliances, e.g., smart refrigerators.

In general, security and privacy issues through the integration of web content in other types of applications has been well documented, and still persist, most notably for different kind of WebView implementations on Android [64], [37], [33]. Studies have also shown differences in the security and privacy posture of different mobile browsers for the Android OS—in particular compared to desktop versions [67], [56]. Whether the same issues exist in – potentially vendor-customized – browsers that ship pre-installed on (Android-based) Smart TVs is an interesting direction for future work.

## X. Conclusions

Our study shows that users are exposed to severe privacy issues in the context of HbbTV-enabled devices. We analyzed the HbbTV traffic of selected European TV broadcasters and observed their adoption of invasive profiling and tracking (third-party) services. Our results show the TV broadcasters' negligence in handling users' data and, in particular, compliance issues with current regulations regarding user consent. Compared to previous studies in Germany, the situation seems not to have evolved over the past five years.

We then performed a user study in Italy to gain insights into their security and privacy awareness. Users seem to have worryingly low awareness of the risks linked to Smart TVs and HbbTV. However, they show great concern when confronted with potential issues—highlighting the need for tools enhancing the security level of the TV viewing experience while also improving the understanding of risks.

As a first step, we propose a solution to mitigate the privacy issues arising from the (essentially unregulated) adoption of HbbTV: HbbTV Blocker. It considers users' need for high customization and ease of use by selectively blocking traffic to known ad and tracking domains.

## Acknowledgements

We thank our anonymous reviewers for their valuable feedback. We also thank Martina Komsic for her help testing additional TV channels, as well as Kevin Borgolte for his feedback on an earlier paper draft.

This research has received funding from the Vienna Science and Technology Fund (WWTF) through project ICT19-056, as well as SBA Research (SBA-K1), a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.

## References

[1] (2020) Samsung Smart-TV Blocklist Adlist (for PiHole). Last accessed: 2022-05-23. [Online]. Available: https://gist.github.com/wassname/b594c63222f9e4c83ea23c818440901b

[2] (2021) Pi-hole Blocklist for Smart TVs. Last accessed: 2022-05-23. [Online]. Available: https://gist.github.com/hkamran80/779019103fcd306979411d44c8d38459

[3] (2021) Smart-TV Blocklist for Pi-hole. Last accessed: 2022-05-23. [Online]. Available: https://perflyst.github.io/PiHoleBlocklist/SmartTV.txt

[4] (2022) Addressable TV | business | equifax. [Online]. Available: https://www.equifax.com/business/product/addressable-tv/

[5] (2022) Auditel - Sintesi Mensile Ottobre 2022. [Online]. Available: https://www.auditel.it/wp-content/uploads/2022/10/Sintesi-Mensile-Ottobre-2022-ts-cum-7.pdf

[6] (2022) Auditel - TV Mediaset.it. [Online]. Available: http://www.mediaset.it/auditel/ascolti.shtml

[7] (2022) Castoola+ adding value to TV ads. [Online]. Available: https://castoola.com/

[8] (2022) Deployments | HbbTV. Last accessed: 2022-05-21. [Online]. Available: https://www.hbbtv.org/deployments/

[9] (2022) EasyList. Last accessed: 2022-05-23. [Online]. Available: https://easylist.to/

[10] (2022) Full survey (in English and Italian). Last accessed: 2022-11-29. [Online]. Available: https://docs.google.com/document/d/1UIsXN0-ihWwqGl4Lju0lEwSbAHvhFG8aniCgLV4m484/

[11] (2022) Garante per la Protezione dei Dati Personali. Last accessed: 2022-05-30. [Online]. Available: https://www.garanteprivacy.it/

[12] (2022) General data protection regulation (GDPR) – official legal text. Last accessed: 2022-05-21. [Online]. Available: https://gdpr-info.eu/

[13] (2022) HiDes UT-100c. Last accessed: 2022-11-29. [Online]. Available: http://http://www.hides.com.tw/product_cg74469_eng.html

[14] (2022) iptables. Last accessed: 2022-11-29. [Online]. Available: https://linux.die.net/man/8/iptables

[15] (2022) mitmproxy. Last accessed: 2022-11-29. [Online]. Available: https://mitmproxy.org/

[16] (2022) Overview | HbbTV. Last accessed: 2022-05-26. [Online]. Available: https://www.hbbtv.org/overview/

[17] (2022) Overview of Pi-hole - Pi-hole documentation. Last accessed: 2022-05-30. [Online]. Available: https://docs.pi-hole.net/

[18] (2022) Pyshark. Last accessed: 2022-11-29. [Online]. Available: http://http://kiminewt.github.io/pyshark/

[19] (2022) Raspberry Pi. Last accessed: 2022-11-29. [Online]. Available: https://www.raspberrypi.org/

[20] (2022) RedOrbit HbbTV Emulator. Last accessed: 2022-11-29. [Online]. Available: https://chrome.google.com/webstore/detail/redorbit-hbbtv-emulator/mmgfafehampkahlmoahbjcjcmgmkppab?hl=en

[21] (2022) RTL 102.5 TV (Page Version ID: 128120211). [Online]. Available: https://it.wikipedia.org/w/index.php?title=RTL_102.5_TV&oldid=128120211

[22] (2022) SoSci Survey. Last accessed: 2022-11-29. [Online]. Available: https://www.soscisurvey.de/

[23] (2022) StevenBlack/hosts. Last accessed: 2022-05-23. [Online]. Available: https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts

[24] (2022) TSDuck. Last accessed: 2022-11-29. [Online]. Available: https://tsduck.io/

[25] (2022) tshark - Manual page. Last accessed: 2022-05-30. [Online]. Available: https://www.wireshark.org/docs/man-pages/tshark.html

[26] (2022) Wireshark - Go Deep. Last accessed: 2022-05-30. [Online]. Available: https://www.wireshark.org/

[27] (2023) CERT.at - Computer Emergency Response Team Austria. Last accessed: 2023-01-16. [Online]. Available: https://cert.at/en/

[28] Y. Aafer, W. You, Y. Sun, Y. Shi, X. Zhang, and H. Yin, "Android SmartTVs Vulnerability Discovery via Log-Guided Fuzzing," in *Proc. of the USENIX Security Symposium (USENIX Security)*, 2021.

[29] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and S. Uluagac, "Peek-a-Boo: I See Your Smart Home Activities, Even Encrypted!" in *Proc. of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2020.

[30] Adintime. TV Audiences 2021. [Online]. Available: https://adintime.com/en/blog/tv-audiences-2021-n128

[31] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaâniche, J.-C. Courrège, and P. Lukjanenko, "Smart-TV Security Analysis: Practical Experiments," in *Proc. of the Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2015.

[32] P. Barre, C. Kasmi, and T. Sabono, "COMMSEC: Hacking into Broadband and Broadcast TV Systems," Hack in the Box Security Conference (HITBSecConf) - Dubai, 2018.

[Online]. Available: https://conference.hitb.org/hitbsecconf2018dxb/sessions/hacking-into-broadband-and-broadcast-tv-systems/

[33] P. Beer, L. Veronese, M. Squarcina, and M. Lindorfer, “The Bridge between Web Applications and Mobile Platforms is Still Broken,” in *Workshop of Designing Security for the Web (SecWeb)*, 2022.

[34] Better Software Group. (2019) HbbTV: What Is it and How Does it Work? Last accessed: 2021-02-17. [Online]. Available: https://bsgroup.eu/hbbtv-what-is-it-and-how-does-it-work/

[35] M. Bozza, “Catch the wave - Hijack HbbTV,” Codemotion, 2019. [Online]. Available: https://www.youtube.com/watch?v=2yeahbhPu9o

[36] P. Cabrera Camara, “SDR Against Smart TVs: URL and Channel Injection Attacks,” DEF CON 27, 2019. [Online]. Available: https://infocondb.org/con/def-con/def-con-27/sdr-against-smart-tvs-url-and-channel-injection-attacks

[37] E. Chin and D. A. Wagner, “Bifocals: Analyzing WebView Vulnerabilities in Android Applications,” in *Proc. of the International Workshop on Information Security Applications (WISA)*, 2013.

[38] E. Chong. (2018) The growing trend of coin miner JavaScript infection. Last accessed: 2021-02-05. [Online]. Available: https://www.fortinet.com/blog/threat-research/the-growing-trend-of-coin-miner-javascript-infection.html

[39] B. Custers, F. Dechesne, A. M. Sears, T. Tani, and S. van der Hof, “A Comparison of Data Protection Legislation and Policies Across the EU,” *Computer Law & Security Review*, vol. 34, no. 2, 2018.

[40] ETSI, “ETSI TS 102 796 V1.5.1, Hybrid Broadcast Broadband TV,” Standard, Sep. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.05.01_60/ts_102796v010501p.pdf

[41] European Audiovisual Observatory. (2016) IRIS Special - Smart TV and Data Protection. [Online]. Available: https://book.coe.int/en/european-audiovisual-observatory/6863-iris-special-smart-tv-and-data-protection.html

[42] European Union Agency for Fundamental Rights, “Your rights matter: Data protection and privacy,” https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection, 2020.

[43] I. Fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, “Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels,” in *Proc. of the Privacy Enhancing Technologies Symposium (PETS)*, 2020.

[44] M. Ghiglieri, “I Know What You Watched Last Sunday - A New Survey Of Privacy In HbbTV,” in *Proc. of the IEEE Web 2.0 Security & Privacy Workshop*, 2014.

[45] M. Ghiglieri and E. Tews, “A Privacy Protection System for HbbTV in Smart TVs,” in *Proc. of the IEEE Consumer Communications and Networking Conference (CCNC)*, 2014.

[46] M. Ghiglieri, M. Volkamer, and K. Renaud, “Exploring Consumers’ Attitudes of Smart TV Related Privacy Risks,” in *Proc. of the International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)*, 2017.

[47] M. Ghiglieri and M. Waidner, “HbbTV Security and Privacy: Issues and Challenges,” *IEEE Security & Privacy*, vol. 14, no. 3, 2016.

[48] R. S. Girons, “HbbTV Country Review,” *HbbTV Symposium*, 2016. [Online]. Available: https://www.hbbtv.org/wp-content/uploads/2017/01/Regis-Saint-Girons-Country-Review-HbbTV-Symposium-2016.pdf

[49] HbbTV Association, “HbbTV 2.0.3 Specification,” Standard, Oct. 2020. [Online]. Available: https://www.hbbtv.org/wp-content/uploads/2020/10/HbbTV-SPEC-00525-HbbTV-SPEC-00515-008-hbbtv203_2020_10_14.pdf

[50] M. Herfurt, “Security concerns with HbbTV,” 06 2013. [Online]. Available: https://www.researchgate.net/publication/277007241_Security_concerns_with_HbbTV

[51] @igorsushko. (2022) TV systems have been hacked for May 9th. [Online]. Available: https://twitter.com/igorsushko/status/1523543444127248385

[52] K. Irion and N. Helberger, “Smart TV and the Online Media Sector: User Privacy in View of Changing Market Realities,” *Telecommunications Policy*, vol. 41, no. 3, 2017.

[53] C. Jensen, C. Potts, and C. Jensen, “Privacy practices of Internet Users: Self-reports versus Observed Behavior,” *International Journal of Human-Computer Studies*, vol. 63, no. 1, 2005.

[54] R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, and G. Vigna, “MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense,” in *Proc. of the ACM Conference on Computer and Communications Security (CCS)*, 2018.

[55] S. Leffel, K. Muller, and J. Kappel, “Addressable TV Advertising,” *smartclip*, 2020. [Online]. Available: https://smartclip.tv/addressable-tv-advertising-white-paper/

[56] M. Luo, P. Laperdrix, N. Honarmand, and N. Nikiforakis, “Time Does Not Heal All Wounds: A Longitudinal Analysis of Security-Mechanism Support in Mobile Browsers,” in *Proc. of the Network and Distributed System Security Symposium (NDSS)*, 2019.

[57] N. Malkin, J. Bernd, M. Johnson, and S. Egelman, “”What Can’t Data Be Used For?”: Privacy Expectations about Smart TVs in the U.S.” in *Proc. of the European Workshop on Usable Security (EuroUSEC)*, 01 2018.

[58] A. M. Mandalari, D. J. Dubois, R. Kolcun, M. T. Paracha, H. Haddadi, and D. Choffnes, “Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic,” in *Proc. of the Privacy Enhancing Technologies Symposium (PETS)*, 2021.

[59] J. Matejka, P. Podhradský, and J. Londák, “Security Manager for Hybrid Broadcast Broadband Architecture Evolution,” in *Proc. of the International Symposium ELMAR*, 2016.

[60] B. Michéle, “Broadcast,” in *Smart TV Security: Media Playback and Digital Video Broadcast*, ser. SpringerBriefs in Computer Science. Springer International Publishing, 2015.

[61] B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, “The Ethics of Algorithms: Mapping the Debate,” *Big Data & Society*, vol. 3, no. 2, 2016.

[62] H. Mohajeri Moghaddam, G. Acar, B. Burgess, A. Mathur, D. Y. Huang, N. Feamster, E. W. Felten, P. Mittal, and A. Narayanan, “Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices,” in *Proc. of the ACM Conference on Computer and Communications Security (CCS)*, 2019.

[63] C. Morgan. Do Android proxy settings apply to all apps on the device? [Online]. Available: http://copyprogramming.com/howto/do-android-proxy-settings-apply-to-all-apps-on-the-device

[64] M. Neugschwandtner, M. Lindorfer, and C. Platzer, “A View to a Kill: WebView Exploitation,” in *Proc. of the USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2013.

[65] Y. Oren and A. D. Keromytis, “From the Aether to the Ethernet - Attacking the Internet using Broadcast Digital Television,” in *Proc. of the USENIX Security Symposium (USENIX Security)*, 2014.

[66] M. T. Paracha, D. J. Dubois, N. Vallina-Rodriguez, and D. Choffnes, “IoTLS: Understanding TLS Usage in Consumer IoT Devices,” in *Proc. of the Internet Measurement Conference (IMC)*, 2021.

[67] A. Pradeep, A. Feal, J. Gamba, A. Rao, M. Lindorfer, N. Vallina-Rodriguez, and D. Choffnes, “Not Your Average App: A Large-scale Privacy Analysis of Android Browsers,” in *Proc. of the Privacy Enhancing Technologies Symposium (PETS)*, 2023.

[68] A. Pradeep, T. M. Paracha, P. Bhomwick, A. Davanian, A. Razaghpanah, T. Chung, M. Lindorfer, N. Vallina-Rodriguez, D. Levin, and D. Choffnes, “A Comparative Analysis of Certificate Pinning in Android & iOS,” in *Proc. of the ACM Internet Measurement Conference (IMC)*, 2022.

[69] S. Preibusch, “Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments,” *International Journal of Human-Computer Studies*, vol. 71, no. 12, 2013.

[70] E. M. Redmiles, Z. Zhu, S. Kross, D. Kuchhal, T. Dumitras, and M. L. Mazurek, “Asking for a Friend: Evaluating Response Biases in Security User Studies,” in *Proc. of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018.

[71] ReVuln. (2013) The TV is watching you: Samsung 0-day. Last accessed: 2021-01-18. [Online]. Available: https://vimeo.com/55174958

[72] L. P. Rondon, L. Babun, K. Akkaya, and A. S. Uluagac, “HDMI-Walk: Attacking HDMI Distribution Networks via Consumer Electronic Control Protocol,” in *Proc. of the Annual Computer Security Applications Conference (ACSAC)*, 2019.

[73] L. P. Rondon, L. Babun, A. Aris, K. Akkaya, and A. S. Uluagac, “Survey on Enterprise Internet-of-Things systems (E-IoT): A security perspective,” *Ad Hoc Networks*, vol. 125, 2022.

[74] J. Rüth, T. Zimmermann, K. Wolsing, and O. Hohlfeld, "Digging into Browser-Based Crypto Mining," in *Proc. of the Internet Measurement Conference (IMC)*, 2018.

[75] L. SeungJin and K. Seungjoo, "Smart TV Security - #1984 in 21st Century," CanSecWest, 2013. [Online]. Available: https://www.slideshare.net/skim71/smart-tv-security-1984-in-21st-century

[76] E. Shiffman. (2018) HbbTV: How addressable TV is implemented in the EU. Last accessed: 2021-03-23. [Online]. Available: https://www.spotx.tv/resources/blog/product-pulse/hbbtv-how-addressable-tv-is-implemented-in-the-eu/

[77] Statista. (2021) Daily TV viewing time in european countries. [Online]. Available: https://www.statista.com/statistics/422719/tv-daily-viewing-time-europe/

[78] ——. (2022) Arte: Audience Market Share Germany 2021. [Online]. Available: https://www.statista.com/statistics/416431/kabel-eins-audience-market-share-germany/

[79] ——. (2022) Austria: TV channels by audience share october 2022. [Online]. Available: https://de.statista.com/statistik/daten/studie/303727/umfrage/marktanteile-der-fernsehsender-in-oesterreich-monatlich/

[80] ——. (2022) Average daily time spent watching TV in the United States from 2019 to 2023. [Online]. Available: https://www.statista.com/statistics/186833/average-television-use-per-person-in-the-us-since-2002/

[81] ——. (2022) Finland: TV channels by audience share 2021. [Online]. Available: https://www.statista.com/statistics/633922/tv-channels-in-finland-by-audience-share/

[82] ——. (2022) Number of TV households worldwide from 2010 to 2026. [Online]. Available: https://www.statista.com/statistics/268695/number-of-tv-households-worldwide/

[83] ——. (2022) Sport1: audience share 2021. [Online]. Available: https://de.statista.com/statistik/daten/studie/285796/umfrage/marktanteil-von-sport-1/

[84] ——. (2022) ZDF: Market Share in Germany 2021. [Online]. Available: https://www.statista.com/statistics/410906/zdf-market-share-germany/

[85] J. Varmarken, H. Le, A. Shuba, Z. Shafiq, and A. Markopoulou, "The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking," in *Proc. of the Privacy Enhancing Technologies Symposium (PETS)*, 04 2020.

## APPENDIX

### A. *Eight Risky Scenarios*

1) The channel you are watching gets information about when and how long you watch it. For broadcasters with multiple channels, there is the possibility that they will merge the information from channels.
2) Your usage habits (i.e., what you use your Smart TV for, when, and how often) are stored by the TV broadcasters. The information collected about you is analyzed to show you personalized (i.e., tailored to you) advertising.
3) Your usage habits (i.e., what you use your Smart TV for, when, and how often) are stored by the TV broadcasters. The purpose and the way such data is stored are not explicitly stated and not certain.
4) Your usage habits (i.e., what you use your Smart TV for, when, and how often) are stored and analyzed by the TV broadcasters.
5) A TV broadcaster offers you the possibility to direct home shopping of the item that is being advertised by simply entering your credentials and credit card information on its website.
6) A TV broadcaster offers you the possibility to direct home shopping of the item that is being advertised by simply entering your credentials and credit card information on its website. It cannot be ruled out that such information is not only received by the broadcaster itself.
7) TV broadcasters may rely on and aggregate data about you coming from bigger services, such as Google and Facebook, to better tailor their content to your preferences.
8) TV broadcasters may rely on and aggregate data about you coming from bigger services, such as Google and Facebook, to better tailor their content to your preferences. This might also be used to show you targeted advertisements. It cannot be ruled out that such information is sold to other parties.

### B. *Coding of Survey Answers*

TABLE VI. CODES DEFINED FOR OPEN-FORMAT QUESTIONS OF THE AWARENESS SURVEY AND WITH THEIR OCCURRENCES IN THE ANSWERS.

| Codes | Answers |
|---|---|
| **Identified Risks** | |
| Privacy (tracking and profiling) | 26 |
| Data and credential leak | 17 |
| Entry point for attackers (TV to access (W)LAN) | 11 |
| Hacking (viruses, broken protocols) | 8 |
| Outdated and vulnerable software/firmware | 4 |
| Access to microphone/camera of the TV | 2 |
| Children accessing not suitable content | 2 |
| Same risks as PCs | 1 |
| Vendors blocking content | 1 |
| **Identified Security Countermeasures** | |
| Firewall or TV in DMZ/separate LAN | 9 |
| Uninstall unused apps and use only trusted ones | 4 |
| Parental control | 3 |
| Block TV webcam and place TV in a "non-sensitive" area | 2 |
| Disable Automatic Content Recognition or Cookies | 2 |
| Data encryption | 2 |
| Antivirus | 2 |
| Two factor authentication for accounts | 1 |
| Block Bootloader | 1 |
| Refreshing MAC address | 1 |
| Buy TV with customer support | 1 |
| Use with care | 1 |
| **What Data is Collected** | |
| Viewing preferences and times | 36 |
| Personal information (date of birth, email address, political orientation) | 10 |
| Geographical location | 4 |
| Credentials | 3 |
| List of installed apps | 3 |
| Purchase related information | 2 |
| TV model | 1 |
| Nearby WiFi networks | 1 |
| Information about devices connected on the same network | 1 |
| Website history | 1 |
| Voice | 1 |
| **Important Features of a Security Tool** | |
| Easy to use and deploy | 28 |
| Customizable (e.g. for expert and non-expert user) | 25 |
| Does not hinder TV experience | 14 |
| Secure | 8 |
| Frequently updated | 4 |
| Provides safe logins (encrypted credentials) | 3 |
| Cheap/Not too expensive | 3 |
| Blocks all tracking | 3 |
| Safe for children | 1 |
| Log of requests | 1 |
| Blocks purchase possibility | 1 |
| Expansible to other smart devices | 1 |

## C. Options for Connecting a Smart TV to the Internet

TABLE VII. FIVE MODES OF CONNECTING A SMART TV.

| **Modality** | Smart TV is connected to the Internet without further precautions | Smart TV is not connected to the Internet | Smart TV is not connected to the Internet and is used as an external monitor for a computer | Smart TV is first secured by you via a protection software before you connect it to the Internet. | Smart TV is secured via preconfigured protection software before you connect it to the Internet |
|---|---|---|---|---|---|
| **Internet Features** | No restrictions | None | Only standard functions of the computer - no updates | No mandatory restriction | No mandatory restriction |
| **Risk** | Potential risks | None | None | None, limited | None, really limited |
| **Additional Effort** | None | None | Computer configured and connected | One-time 15 min. for configuration | None, since preconfigured |
| **Additional Cost** | None | None | None | One time 20€ | One time 40€ |

## D. Sample of Extracted HbbTV URLs

TABLE VIII. HBBTV START URLS FOR 9 ITALIAN CHANNELS.

| **Channel Name** | **Start Link (URLs)** |
|---|---|
| Sportitalia | http://www.sportitalia.kbbtv.tech/hbbtv/sportitalia/sportitaliachannel/index.html |
| RDS | http://hbbtv.rds.radio |
| RealTime | http://discovery.castoola.tv/realtime |
| RTL | https://cloud.rtl.it/hbbtv.rtl.it/rtlchannel/index.html |
| Rai 1 | https://www.raiplay.it/hbbtv/launcher/RemoteControl/index.html?delivery=2<br>https://www.raiplay.it/hbbtv/RaiPlay2020/index.html |
| Spike | http://www.kbbtv.tech/viacom/viacomchannel/index.html |
| Canale 5 | http://hbbtv.mediaset.net/app/mplayhbbtvgold/backdoor.shtml<br>http://hbbtv.mediaset.net/app/mplayhbbtvgoldzoo/dev/index.html<br>https://mhptivu.mediaset.net/app/mplayhbbtvtivu/index.html<br>https://tivuon-hbbtv-lativu.tivu-alchemy.net/index.html?configuration=prod |
| La7 | https://ht.la7.it/index.php |
| Radio Kiss Kiss | http://www.kisskiss.kbbtv.tech/hbbtv/kisskisschannel/index.html |
| Radio Libertà | https://hbbtv.persidera.it/hbbtv/jump/index.html?channelId=38893 |
| BOM Channel | http://95.110.225.170/hbbtv_bootstrap/index.php |
| NOVE | http://discovery.castoola.tv/nove |
| Caccia e Pesca | https://app.cacciaepesca.tv/hbbtv-cp/ |
| QVC | http://qvc-italy-hbbtv-app.qvc-italy.c.nmdn.net/redbutton |
| TeleNordEst | http://hbbtv.tdbnet.it/run.php?pid=2049 |
| TeleChiara | http://iphd.it/hbbtv/telechiara/index.php |
| SuperTennis | https://hbbtv.persidera.it/hbbtv/launcher/index.html?appId=25970 |
| LineaGem | http://www.grupposciscione.kbbtv.tech/hbbtv/lineagem/index.php |
| Warner TV | http://it.container.enhanced.live/warnertv/ |
| TV 8 | https://data-hip-gcdn-skycdn-it.akamaized.net/iapp/produzione/hbbtv/Addressable/index.html |