Abstract—The DVB standard does not mandate the use of authentication and integrity protection for transport streams. This allows malicious third parties to replace legitimate broadcasts by overpowering terrestrial transmissions. The rogue signal can then deliver a malicious broadcast stream to exploit security vulnerabilities on Smart TVs (STV) in range. We implemented a proof-of-concept attack based on a malicious HbbTV app, able to acquire permanent system-level access to a STV over the air, in less than ten seconds. These attacks, however, are severely limited in range due to required co-channel protection ratios (CCPR), which is in direct contradiction to previous publications. We present evidence for these limitations in form of lab experiments, extensive simulations, and field measurements. To this end, we developed an automated, low-cost method for CCPR determination, as well as a method for non-disruptive attack range measurements based on a gap filler and the resulting channel impulse response.

Index Terms—DVB-T, HbbTV, security, Smart TV, CCPR.

I. INTRODUCTION

DURING the last decade, many countries have completed the transition from analog to digital television (DTV). Now, more than a billion households have access to DTV services [1]. Broadcasters in Europe and around the world employ the Digital Video Broadcasting (DVB) standard. DTV has also enabled the introduction of interactive TV services. One of these services is Hybrid Broadcast Broadband TV (HbbTV) [2], which has been adopted in 25 countries. HbbTV builds upon existing web standards, which allows vendors to leverage existing code to implement runtimes and developers to rapidly roll out applications. Current Smart TVs (STV) have built-in support for HbbTV, which has led to high acceptance among consumers.

The DVB and HbbTV standards, however, do not mandate the use of authentication and integrity protection for transport streams and applications, respectively. This allows malicious third parties to impersonate broadcast stations, which in turn can be abused to deliver and launch arbitrary HbbTV apps. A malicious HbbTV app can exploit (vendor-specific) security vulnerabilities on the STV and thereby permanently gain full control over the device. STVs have become an attractive target due to powerful hardware, connection to (private) local networks and the Internet, and their widespread use. To demonstrate the feasibility of such attacks, we implemented a fully functional proof-of-concept (PoC) attack. The PoC overpowers a regular DVB-T broadcast with a signal that contains a malicious HbbTV app. This app is automatically started on the STV and then gains full control by exploiting a vulnerability in the STV’s media playback system. The attack and subsequent infection do not require any user interaction and are invisible to victims.

There are, however, significant limitations to broadcast-originated attacks, both in terms of range and stealthiness. Previous publications [3], [4] have calculated the attack range solely based on (free-space) path loss, ignoring required co-channel protection ratios (CCPR). Taking into account the CCPR, however, results in a significantly reduced attack range. Furthermore, the resulting co-channel interference (CCI) creates a huge mush area, in which neither signal can be received. These customers—cut off from broadcast service—are likely to file complaints, which significantly limits the presumed stealthiness of such an attack.

This work presents range and mush zone estimations that take into account required CCPRs, along with extensive simulations for an area in Los Angeles. These results have been validated both in the lab and in field experiments. We also present an automated, low-cost method to measure CCPRs on modern STVs together with the obtained results. Furthermore, this work presents a novel method to determine attack ranges in the field, without disrupting the regular broadcast delivery.

The rest of the paper is organized as follows. Section II provides the necessary background for the following sections. Section III describes the attack surface of a modern Smart TV. Section V presents our broadcast-assisted attack and the PoC implementation. Section V explores the limitations to our attack, both in terms of range and detectability. Section VI provides the results of our attack simulations. Section VII introduces a novel approach to determine attack ranges in the field based on a gap filler and the resulting channel impulse response. Finally, Sect. VIII closes with the conclusion.

II. BACKGROUND

This section provides the background on the technologies and previous publications related to this work.

A. HbbTV

Hybrid Broadcast Broadband Television (HbbTV) [2] allows broadcasters to augment their TV programs with interactive applications. HbbTV includes information on available applications in the DVB transport stream. Every program can have several associated applications, one of which is started automatically upon selection of the respective program. In general, this so-called red button application is supposed to
The current STV ecosystem, however, is particularly ill-suited to STVs and subsequently to connected networks and devices. Can be abused by attackers to gain unauthorized access to vulnerabilities. If they are not patched by the vendor, they is implemented in open source libraries from third parties. Privileges. This application runs multiple threads to provide the user interface, apps, media playback, etc.; much of which is implemented in open source libraries from third parties.

Software projects of this size tend to contain exploitable vulnerabilities. If they are not patched by the vendor, they can be abused by attackers to gain unauthorized access to STVs and subsequently to connected networks and devices. The current STV ecosystem, however, is particularly ill-suited for guaranteeing a secure software stack.

First and foremost, the STV's system software—the firmware—cannot be updated incrementally; instead, up to several-hundred megabytes have to be downloaded and installed for every update, however small. This severely limits the work is purely theoretical. They did not overpower an existing channel but instead connected a modulator directly to the STV. The presented range calculations thus ignore required CCPRs, leading to an underestimated attack coverage by orders of magnitude. This is explained in detail in Sect. V.

III. SMART TV ATTACK SURFACE

Virtually all Smart TVs employ a Linux-based operating system. Many STV models implement most of the functionality in a single proprietary application with unrestricted system privileges. This application runs multiple threads to provide the user interface, apps, media playback, etc.; much of which is implemented in open source libraries from third parties.
the rate at which firmware updates can be deployed, especially in terms of user acceptance. Furthermore, STV vendors introduce a variety of devices each and every year, which makes it increasingly difficult to supply current and old models with (timely) updates. In combination with open source software (OSS), this becomes a real problem. STV vendors have to rigorously monitor security announcements for all of the libraries in use on current and previous STV models. Any newly discovered vulnerability entails a time-consuming firmware development, testing, and deployment process. As a result, legacy STV models are cut off from updates, and current models suffer from delayed updates leading to potentially vulnerable devices.

Additional bugs can be identified in proprietary software by reverse engineering or fuzzing. Attackers can target all of these vulnerabilities. Their exploitation is comparatively easy, as many STVs lack security best practices established in the PC world. Privilege separation, sandboxing, and exploitation countermeasures such as DEP and ASLR \[14\] have only recently begun to see a more widespread deployment. An attacker controlling the broadcast channel can exploit vulnerabilities in the HbbTV runtime, the media playback, and the components related to broadcast processing.

A. HbbTV Runtime

HbbTV apps are written in CE-HTML (or HTML5 for HbbTV 2.x) and therefore most runtimes are based on existing web browser projects. A popular example is WebKit, which is used by several STV vendors to implement HbbTV. New vulnerabilities in web runtimes, however, are discovered and published regularly, leading to frequent updates on the PC platform. Fig. 1 shows the number of code execution vulnerabilities reported for WebKit during the past five years. On STVs, however, these updates have to be incorporated into the firmware, leading to substantial delays. In the case of legacy devices, the frequency at which firmware updates are developed decreases and eventually stops completely. Fig. 2 illustrates this with devices from three popular STV vendors: After a period of five years, firmware updates essentially cease to be published.

B. Media Playback

STVs employ a central component for media retrieval, analysis, decoding, and display—the media playback system. This system is used by other STV components such as apps, the HbbTV runtime, and the built-in media player. Several STV vendors use open source libraries to implement the media handling, e.g., FFmpeg, GStreamer, or libstagefright \[15\]. Handling media files, however, is a complex task, which has resulted in the continuous discovery of vulnerabilities (see Fig. 1). These vulnerabilities can be exploited on STVs at large scale, as we have previously demonstrated for STVs employing FFmpeg \[11, 12\]. Further vulnerabilities have recently been discovered in libstagefright, the media playback system of Android devices \[16, 17\], and in GStreamer \[18\]. Table 1 lists open source media processing frameworks used on several popular STVs.

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
<th>Released</th>
<th>Vendor</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFmpeg</td>
<td>SVN-r158**</td>
<td>11.2008</td>
<td>A</td>
<td>2009</td>
</tr>
<tr>
<td></td>
<td>SVN-r19089</td>
<td>05.06.2009</td>
<td>A</td>
<td>2010</td>
</tr>
<tr>
<td></td>
<td>0.6.90-rc</td>
<td>03.04.2011</td>
<td>A</td>
<td>2011</td>
</tr>
<tr>
<td></td>
<td>n1.0</td>
<td>28.09.2012</td>
<td>B</td>
<td>2012</td>
</tr>
<tr>
<td></td>
<td>SVN-r17783</td>
<td>03.03.2009</td>
<td>B</td>
<td>2013</td>
</tr>
<tr>
<td></td>
<td>0.6.1</td>
<td>18.10.2010</td>
<td>C</td>
<td>2014</td>
</tr>
<tr>
<td></td>
<td>n1.1.1</td>
<td>20.01.2013</td>
<td>D</td>
<td>2014</td>
</tr>
<tr>
<td>GStreamer</td>
<td>0.10.36</td>
<td>20.02.2012</td>
<td>B</td>
<td>2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C</td>
<td>2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>2015</td>
</tr>
<tr>
<td>Stagefright</td>
<td>1.2</td>
<td>12.02.2013</td>
<td>D</td>
<td>2014</td>
</tr>
</tbody>
</table>

TABLE I: Media playback libraries used on Smart TVs

C. Service Information

DVB defines a number of service information (SI) tables \[19\], which are delivered in the broadcast transport stream and are processed by the Smart TV. If the processing software contains vulnerabilities, this may be exploited by transmitting maliciously crafted tables. Vulnerable implementations of the DVB subtitling system \[20\] could be attacked similarly. With the ongoing consolidation of STV hardware platforms and associated software stacks, a single vulnerability in this component can potentially affect several STV vendors and a wide variety of devices.

IV. BROADCAST-ASSISTED ATTACKS

The DVB standards do not require broadcasts to be authenticated. As a result, receivers are unable to distinguish between authentic and forged broadcasts. Malicious third parties can abuse this to alter the received programming.

In the past, however, this was not considered a serious threat, as the potential damage was limited to disseminating fake alerts, advertisements, etc. However, this has changed with the introduction of Smart TVs and interactive digital services such as HbbTV. An attacker controlling the broadcast channel is able to deliver malicious applications to receivers, in particular STVs. Combined with vulnerable system software on STVs, this can become a real threat for STV owners.

Compromising a STV consists of two main parts. First, the broadcast channel has to be controlled, i.e., for terrestrial broadcasts, victim STVs must receive the rogue signal instead of the regular signal. Second, the rogue signal must contain malicious code to take over victim STVs, e.g., a malicious HbbTV application (see Sect. III). Limitations to this attack are discussed in detail in Sect. IV. This section is based on our previous work \[12\].

A. Rogue DVB-T Signal

An attacker has to overpower the regular DVB-T or DVB-T2 signal arriving at the receiver; both are vulnerable and we will thus refer to them as DVB-T. Several attack scenarios are conceivable: The targeted, the untargeted small range, and the regional repeater scenario. In the targeted scenario, the STV of a specific person of interest is compromised, using a highly
directional antenna. For the small range scenario, all TVs in the vicinity of the attacker’s transmitter are the target.

In some ways, this attack can be compared to man-in-the-middle (MITM) attacks in GSM networks [21]. The GSM specification requires that mobile stations (MS) authenticate to the network, but not vice versa. In DVB-T, broadcast stations do not authenticate to receivers, either. The use of allocated frequencies, however, differs between the two systems. In GSM, the base stations (BS) in the vicinity of the MS operate on different frequency bands and the MS connects to the BS with the strongest signal. An attacker can therefore operate a rogue BS on an unused frequency, i.e., there is no need to physically overpower another BS on the same channel. DVB-T receivers, on the other hand, remain tuned to the frequency of the currently selected channel, thus forcing an attacker to overpower the regular broadcast signal. As opposed to MITM attacks in the GSM network, this creates an area without proper reception of either signal, which we refer to as the mush zone (see Sect. V-A).

Another interesting target for attackers is broadcast relay stations or gap fillers [22]. Here, an attacker overpowers the regular broadcast signal at the receiving antenna of the retransmission station, provided the signal is picked up off-air. This allows the attacker to abuse the amplification service of the retransmission station and hence reach a large region.

1) **Satellite and Cable**: A resourceful attacker can attempt to overpower a satellite up- or downlink, both of which has occurred repeatedly in the past [23]. Cable television systems can also be attacked, by injecting malicious signals into distribution lines. Even worse, an attacker could target cable TV headend facilities that are fed by satellite or terrestrial signals. The attacker-controlled signal is then distributed through the headend to a large amount of cable subscribers.

2) **Proof of Concept**

Our proof-of-concept (PoC) implementation demonstrates that broadcast-assisted attacks are feasible in practice and can pose a threat to consumers, which helps vendors and standard bodies to understand the risks and develop countermeasures. Furthermore, being able to analyze an attack in practice gives us the opportunity to identify weak spots, both on the side of the target and the attacker, and design efficient countermeasures. It also allows us to verify to what degree previously proposed attacks are feasible in practice. Figure 3 illustrates the MITM attack scenario that was chosen for the PoC implementation. The regular terrestrial broadcast signal is picked up, modified to include a malicious HbbTV app, and retransmitted. STVs in range receive this signal and automatically execute the HbbTV app, thereby infecting themselves with persistent malware. It is important to note that no user interaction is required and the STV compromise is invisible to the victims.

1) **Regular Signal Acquisition**: Retransmission of the current program is required for a stealthy—invisible to the user—attack. The transport stream is acquired in real-time with a cheap USB-based, consumer-grade DVB-T receiver. Standard Linux tools are used to tune the receiver to the target station and acquire the raw transport stream, as shown in Listing 1.2

2) **Transport Stream Modification**: The transport stream is modified to automatically launch the malicious HbbTV app on victim STVs. This does not require any user interaction, i.e., the user does not have to change the channel or stop a currently active HbbTV app. The HbbTV specification states that a running app can be killed via the broadcast signal by including both the original and the added malicious app with a new ID. In addition, the type is set to PRESENT and AUTOSTART for the original and malicious app, respectively. The STV thus kills the running app and immediately starts the malicious app. These modifications were performed with the open source tool collection OpenCaster from Avalpa [24] (see Listing 1.1).

**Listing 1: Signal acquisition and modification** [12]

```
1 # tune to station
dvbsnoop -b -s ts -tsraw > reg.ts &
2 # grab and save raw transport stream
tzap -r 'Das_Erste' &
3 # replace ait and object carousel
tsmodder reg.ts +2070 ait.ts +2171 oc.ts > rogue.ts
4 dvbsnoop -b -s ts -tsraw > reg.ts &
5 # replace ait and object carousel
tsmodder reg.ts +2070 ait.ts +2171 oc.ts > rogue.ts
```

**TABLE II: USB-based DVB-T transmitter options (RF power for DTU-215 from vendor specification)** [12]

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Model</th>
<th>Type</th>
<th>Power [dBm]</th>
<th>Price [$]</th>
</tr>
</thead>
<tbody>
<tr>
<td>DekTec</td>
<td>DTU-215</td>
<td>DVB-T/C</td>
<td>(-15)</td>
<td>1,600</td>
</tr>
<tr>
<td>Hides</td>
<td>UT-100C</td>
<td>DVB-T</td>
<td>8</td>
<td>150</td>
</tr>
<tr>
<td>G.S.G.</td>
<td>HackRF</td>
<td>DVB-T</td>
<td>-7</td>
<td>300</td>
</tr>
<tr>
<td>Ettus</td>
<td>USRP B210</td>
<td>SDR</td>
<td>10.5</td>
<td>1,100</td>
</tr>
</tbody>
</table>

**Fig. 3: Regular broadcast is picked up (1), modified to include malicious HbbTV app and retransmitted (2), invokes compromising media playback on target STVs (3), and finally executes payload, e.g., camera tapping (4). Note the shaded mush area, where neither signal has sufficient co-channel protection to be received properly (not to scale, cf. Fig. 7).**
profession, and overall signal quality are provided in Table II and Fig. 4. We used the cost-efficient UT-100C for the majority of the experiments.

b) Isolation: A MITM attack requires a setup that is able to receive, modify, and retransmit the regular signal in real-time. The required level of isolation between the receiving and transmitting antenna is difficult to achieve without expensive professional equipment. In practice, however, there are several ways to solve this problem. An attacker can receive the regular signal outside of the mush zone and then use an out-of-band mechanism, e.g., the Internet, to deliver the broadcast stream to the rogue transmitter. Alternatively, if the station is broadcasting publicly available material such as an old movie, the attacker does not need to operate a receiver. Finally, the attack can be launched during commercial breaks, where the regular broadcast can be replaced with arbitrary commercials.

3) Malicious App: An HbbTV app is delivered either via HTTP(S) or the DSM-CC object carousel (see Sect. II-A2). Experiments with our PoC attack show that the HTTP(S)-based delivery is generally faster and that it is the only method to allow for media playback exploits. The total time required for an attacker to be on air to compromise a STV is less than ten seconds.

4) Exploitation: Our PoC attack exploits a vulnerability in the media playback system (see Sect. III-B). A malicious video file is included in the HbbTV autostart app, which is automatically started when the (invisible) app launches on the STV. The vulnerability is triggered upon playback, which results in a root shell on the STV. The video itself is never actually displayed and therefore does not interrupt the currently running broadcast. The final step after having gained access to the STV is the execution of malicious payload. Our PoC exploit establishes a connection to a remote server, which is used to load and run arbitrary code on the STV. For demonstration purposes, our code taps into the STV’s camera and microphone and transmits the recorded stream over the Internet in real-time.

5) Disclosure and Reaction: We initially contacted the HbbTV association in June 2014 to responsibly disclose our findings on HbbTV-assisted attacks. We renewed this offer in August, which led to a live demonstration on a real device to the HbbTV Chairman in September. We have since been invited to demonstrate and discuss our results and possible countermeasures at various meetings of the HbbTV group, and also the DVB Technical Module for terrestrial broadcasts (DVB-TM-T) in January 2015. This collaboration has raised a thorough awareness for HbbTV-assisted attacks within the HbbTV and DVB group, and has created an active process to specify future protection measures. In May 2015, the HbbTV group announced that they were working closely with the DVB group and that they had decided on an approach based on the authentication of critical MPEG-2 sections. An updated specification protecting against the HbbTV-assisted malware delivery presented in this work is expected to be completed in early 2017.

V. LIMITATIONS

The presented attack is subject to a number of limitations, most notably in terms of range and stealthiness. This section is the extended version of our work published in [12], expanding the measurements for DVB-T and adding results for two DVB-T2 modes in active use.

A. Co-Channel Protection Ratio

The attack scenario consists of a regular terrestrial broadcast and a rogue transmitter broadcasting on the same channel, thus overpowering the signal in its vicinity. In this co-channel situation, only the stronger of the two signals can be decoded while the other appears as co-channel interference (CCI). More precisely, the stronger signal can be decoded if its power ratio w.r.t. the weaker signal exceeds a certain threshold — the co-channel protection ratio (CCPR).

The required CCPR depends on the transmission’s modulation type and forward error correction (FEC), given as code rate (CR). If the actual ratio drops below the CCPR, neither signal will be decoded and the TV screen turns dark. The attack therefore creates three distinct areas of signal coverage: First, the area surrounding the rogue transmitter, in which the rogue signal strength exceeds the required CCPR w.r.t. the regular broadcast signal. Surrounding this area is a second area, in which neither signal is strong enough to achieve the required CCPR and TV screens thus turn dark.
We will call this the mush area, adopting a term used in mediumwave broadcasting to describe areas with echo-like interferences. And finally the remaining areas serviced by the regular broadcast signal, exceeding the required CCPR w.r.t. the rogue signal.

1) Measurements: Broadcasters aim to provide high-quality service and thus target C/N ratios that allow for "Quasi Error Free" (QEF) transmissions [22]. The C/N ratio required for an attack, however, is lower. Victim receivers must lock on to the signal for at least ten seconds, which is enough to decode the AIT and launch the malicious application. This is the evaluation criterion we chose for measuring CCPRs related to the attack scenario.

To determine the CCPR for all (8 MHz channel) DVB-T variants, we implemented an automated measurement setup as illustrated in Fig. 5a. It consists of two low-cost transmitters, a target TV, and a laptop controlling the measurements and reading serial output from the TV—alternatively, HbbTV requests can be used for the feedback channel if no serial output is available. Both of the transmitters use the same settings for modulation and CR. They are placed close to the STV’s antenna and have a direct line-of-site connection, resulting in an AWGN propagation channel. One of the transmitters simulates the regular broadcast and transmits with a low, fixed power. The second transmitter serves as the rogue station, starting with sufficiently higher power output, which is subsequently decreased by 1 dB in each step. During each step, the TV’s serial output is monitored for changes in the signal lock status of its receiver. The measurement setup is able to determine CCPR values by associating the relation between the regular and rogue station’s power and the three states mentioned above: Rogue broadcast, mush zone, and regular broadcast. If the receiver is able to maintain a steady signal lock for a period of ten seconds, the current CCPR is deemed sufficient to launch a successful attack; otherwise, an attack with this CCPR will result in mush zone. Figure 5b illustrates the signals decoded by the STV depending on the rogue transmitter power $P_{rogue}$. All measurements were repeated ten times and cross-checked on a different STV model. Neither the guard interval (GI) nor the transmission mode (2K or 8K) had a significant influence on the measured CCPRs. The resulting CCPR values are given in Table II as M2.

For comparison, we measured the minimum required C/N ratio conforming to the Subjective Failure Point (SFP) assessment method [28]. A Rohde & Schwarz SFU was used to generate the broadcast signal, add noise, and apply the channel simulation. The signal was fed to a 2015 STV model, the Samsung UE40JU6450, which was used to assess the picture quality. The results are labeled as M1 in Table II and Table IV. The latter provides results for two DVB-T2 variants in active use by German broadcasters, labeled G2 (16Kc, 64-QAM, CR 3/5, GI 19/128, PP2, LDPC 64800, SISO) and G8 (32Kc, 64-QAM, CR 2/3, GI 1/16, PP4, LDPC 64800, SISO) [29]. Additional values obtained from simulations are provided for DVB-T2 by DTVP [22, Annex A].

Reimers et al. [26, Table 11.7] and ETSI [27, Table A.1] provide carrier-to-noise (C/N) ratios required to achieve a quasi-error-free (QEF) DVB-T transmission, i.e., less than one uncorrected error event per hour [22]. ITU-R provides measured CCPR values for a wanted DVB-T signal that is interfered with by another DVB-T signal [28, Table 15]. The values are chosen such that a QEF transmission is achieved, including a typical implementation margin.

Compared to our measurements, the values from ETSI and ITU are roughly 1 dB and 3 dB higher, respectively; the values calculated by Reimers are slightly higher than the values measured by us and slightly lower than the values given by ETSI (with the exception of 64-QAM and CR 1/2). Reimers, ETSI, and ITU target QEF transmissions, whereas our measurements reflect the minimum CCPR required to launch a successful attack.

2) Attack Range and Controlled Area: The Log-Distance path loss model [30] reflects that the average received signal power decreases logarithmically with the distance. This is accounted for by a path loss exponent $n$ that describes the rate at which the signal power decreases. In free space, for instance, $n$ equals 2, whereas obstructions will increase the value of $n$. The resulting large-scale average path loss in decibel for a distance $d > d_0$ between a transmitter and receiver is

$$PL(d) = PL(d_0) + 10n \log_{10} \left( \frac{d}{d_0} \right)$$

(1)

where $PL(d_0)$—or $PL_0$—is the reference path loss, i.e., the average path loss at a reference distance $d_0$. $PL_0$ is calculated either by using the formula for free-space path loss (FSPL) [30] or by actual field measurements at $d_0$. Two locations with the same distance $d$ from the transmitter, however, may vary in the amount of surrounding environmental clutter. The corresponding signal levels may therefore differ significantly from the average value. This effect—log-normal shadowing [30]—can be accounted for by adding a zero-mean, Gaussian-distributed random variable $X_\sigma$ with standard deviation $\sigma$

$$PL(d) = PL(d_0) + 10n \log_{10} \left( \frac{d}{d_0} \right) + X_\sigma.$$  

(2)

Since an attacker is generally more interested in covering the largest possible area than its exact shape, we will ignore log-normal shadowing and thus assume $X_\sigma = 0$. To estimate the impact of a small-range attack as described in Sect. IV-A—an attacker targets all STVs in the vicinity—it is important to assess the size of the area controlled by an attacker with a rogue transmitter and low-power amplifier. For a TV to be able to receive a wanted signal in the presence of an unwanted signal, the CCPR of the wanted signal, $\alpha_{wanted}$, has to be taken into account so that the following condition regarding the received power at the TV’s input is met:

$$P_{r, wanted} \geq P_{r, unwanted} + \alpha_{wanted}.$$  

(3)

Here, the wanted and unwanted signals are the rogue and regular signal, respectively, and (3) thus becomes

$$P_{r, rogue} - PL(d_{rogue}) \geq P_{r, reg} - PL(d_{reg}) + \alpha_{rogue}.$$  

(4)

In general, it can be assumed that the power radiated by the regular broadcast station is much higher than that of the rogue station, i.e., $P_{r, reg} \gg P_{r, rogue}$. An attacker will therefore have
A rogue signal can be calculated as the rogue transmitter at which TVs will be able to receive the broadcast station is weak, i.e., $P_{\text{rogue}} < P_{\text{reg}}$, for reasons of simplification we will assume that $P_{\text{reg}}$ is constant in the area under attack. Using (2), the maximum distance $d_{\text{rogue}}$ from the rogue transmitter at which TVs will be able to receive the rogue signal can be calculated as

$$P_{\text{rogue}} - P_{\text{reg}} - 10n\log_{10}\left(\frac{d_{\text{rogue}}}{d_0}\right) \geq P_{\text{reg}} + \alpha_{\text{rogue}}$$

$$10n\log_{10}\left(\frac{d_{\text{rogue}}}{d_0}\right) \leq P_{\text{rogue}} - P_{\text{reg}} - \alpha_{\text{rogue}} - P_L$$

$$d_{\text{rogue}} \leq d_0 \cdot \frac{\lambda}{4\pi d_0}\cdot 10^{\frac{P_{\text{reg}} - P_{\text{rogue}} - \alpha_{\text{reg}}}{10}}$$

For FSPL up to $d_0$, (7) becomes

$$d_{\text{rogue}} \leq d_0 \left(\frac{\lambda}{4\pi d_0}\right)^{\frac{2}{n}} \cdot 10^{\frac{P_{\text{reg}} - P_{\text{rogue}} - \alpha_{\text{reg}}}{\text{SNR}}}$$

Finally, the attacker-controlled area is

$$A_{\text{rogue}} = \pi d_{\text{rogue}}^2$$

TABLE III: CCPR measured according to the method presented in Sect. V-A1 (M2) and minimum required $C/N$ measured with professional equipment (M1) vs. calculated $C/N$ values from Reimers et al. [26] Table 11.7 (Reim.) and ETSI [27] Table A.1 vs. CCPR by ITU-R [28] Table 15. Values are given in dB for Gaussian, Ricean, and Rayleigh propagation channels

<table>
<thead>
<tr>
<th>DVB-T2 variant</th>
<th>Gauss</th>
<th>Rice</th>
<th>Rayleigh</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>M1</td>
<td>M2</td>
<td>ETSI</td>
</tr>
<tr>
<td>G2</td>
<td>12.8</td>
<td>14.8</td>
<td>13.3</td>
</tr>
<tr>
<td>G8</td>
<td>14.1</td>
<td>15.7</td>
<td>14.7</td>
</tr>
</tbody>
</table>

TABLE IV: Min. required $C/N$ [dB] for DVB-T2 variants G2 (16QAM CR3/5 PP) and G8 (32QAM CR2/3 PP4), measured (M1) and simulated (DTVP) [29].
A few simplifications are made. An attacker will target an area that is rather far away from the regular station, due to the significantly smaller power output of the rogue station. At this distance and for the comparatively small area affected by the rogue station, it will be assumed that the signal strength of

\[ P_{t,\text{rogue}} = P_{t,\text{reg}} - 20 \log_{10} \frac{d_0}{d} \]

and that the attacker uses an omnidirectional antenna. As a result, the shape of the attacker-controlled area and the mush zone is a circle and an annulus, respectively.

In general, the signal strength of the rogue transmitter’s signal strength cannot maintain the required CCPR \( \alpha_{\text{rogue}} \) w.r.t. the regular signal, and extends to where it has become so weak that the regular signal achieves the required CCPR \( \alpha_{\text{reg}} \), i.e., \( d_{\text{rogue}} < d_{\text{mush}} < d_{\text{reg}} \). If both signals share the same modulation type and code rate, the mush zone corresponds to twice the CCPR. If they use different parameters, this is the sum of both CCPRs (cf. Fig. 7). The ratio between the radii \( d_{\text{rogue}} \) and \( d_{\text{reg}} \) of the attacker-controlled and attacker-affected area, respectively, can be calculated using (7) as

\[ d_{\text{rogue}} = d_0 \cdot 10^{-\frac{\alpha_{\text{rogue}}}{n} + c} \]

(10)

\[ d_{\text{reg}} = d_0 \cdot 10^{-\frac{\alpha_{\text{reg}}}{n} + c} \]

(11)

\[ \frac{d_{\text{rogue}}}{d_{\text{reg}}} = 10^{-\left(\frac{\alpha_{\text{rogue}} + \alpha_{\text{reg}}}{2n}\right)} \]

(12)

This means that the ratio between the two radii only depends on the corresponding CCPRs and the PLE \( n \). The regular broadcast’s CCPR \( \alpha_{\text{reg}} \) cannot be influenced by the attacker, whereas the rogue signal’s CCPR \( \alpha_{\text{rogue}} \) can be influenced to some degree as described in Sect V-C. Using (12), the relation between attacker-controlled and attacker-affected area becomes

\[ \frac{A_{\text{controlled}}}{A_{\text{affected}}} = \frac{\pi d_{\text{rogue}}^2}{\pi d_{\text{reg}}^2} = \left( \frac{d_{\text{rogue}}}{d_{\text{reg}}} \right)^2 = 10^{\left(\frac{\alpha_{\text{rogue}} + \alpha_{\text{reg}}}{2n}\right)} \]

(13)

Overpowering a 16-QAM, CR 2/3 broadcast thus creates a mush area 99 times the size of the attacker-controlled area, assuming an FSPL propagation model \( (n = 2) \). This is a huge
Fig. 8: Percentage of attacker-controlled area out of total attacker-affected area, for various PLEs \( n (d_0 = 1 \text{ m}) \). Regular station uses 16-QAM and 64-QAM with CR 2/3 \((\alpha_{\text{reg}} = 10 \text{ dB and } 15 \text{ dB})\); rogue station uses identical settings \((\alpha_{\text{rogue}} = \alpha_{\text{reg}})\) and the most robust settings, i.e., QPSK with CR 1/2 \((\alpha_{\text{rogue}} = 2.5 \text{ dB})\)\[12\]
collateral damage and greatly reduces the stealthiness of the untargeted terrestrial attack. Figure 8 shows the percentage of attacker-controlled area for various PLEs \( n \) and CCPRs \( \alpha_{\text{rogue}} \); the corresponding remaining area is the mush zone.

C. Variations
An attacker can increase the controlled area by decreasing the required CCPR \( \alpha_{\text{rogue}} \), i.e., choose a more robust modulation and code rate. QPSK with CR 1/2 yields the greatest robustness, requiring a CCPR of only approximately 2.5 dB as compared to, e.g., 10 dB for 16-QAM with CR 2/3 (cf. Table III). The drawback is a reduced available bitrate (factor three for the above example)\[27\]), which cannot accommodate the original transport stream. The attacker either has to decrease the A/V quality by using a higher compression level or remove other elementary streams or programs from the transport stream, both of which increases the risk of being detected.

VI. ATTACK SCENARIOS

Three different practical attack cases are discussed in this section based on digital terrestrial television coverage simulations on a specific area.

A. Attack Scenarios and Associated Characteristics
The area under analysis is a big urban area of 11 km x 15 km located in Los Angeles and selected from a larger region that includes the broadcaster’s location. One and two story houses prevail in this flat region surrounded by terrain heights that range from a few tens to several hundred meters. In fact, the height of the transmitter considered for the simulations was 1745 meters above sea level. Fig. 9 shows the orography of the terrain as well as the LoS from the transmitter.

Table V contains a description of each one of the scenarios under study. They have been proposed to take into account the most influential factors for a successful attack situation.

The scenarios under analysis differentiate three subcases according to the reception mode used by potential victims. There will be cases where the terrestrial service is received using a rooftop antenna. This case is typical in countries where the terrestrial platform is the dominant delivery method in Europe.

There is a second scenario where the DTV consumers receive the service indoors. This is a common trend in American and Asian countries.

A third case involves a gap-filler and provides the opportunity for an attacker to target all receivers within the DTV gap-filler coverage area.

![Fig. 9: Simulation area](image)

The study differentiates several options for the rogue signal. The attacker has two options, one of which is to use the same mode as the broadcaster. This way the rogue signal equals the desired service capacity. On the negative side (for a potential attacker) the SNR and protection ratio values have to be similar. The second option is to use a more robust mode, requiring a less demanding threshold (SNR and protection ratio) and thus providing a better scenario for the attacker. This option limits the bit rate available to the rogue service (see Sect. V-C).

Finally it should be highlighted that the users that are most likely to be potential victims (in terms of simplicity from an attacker’s perspective) are those that receive the DTV service without employing active amplifiers on their reception infrastructure. If the receiving system is based on amplifiers, the new superimposed signal (rogue signal) on the desired service is likely to drive the amplifier into the saturation region. This will lead to service degradation or loss, thereby decreasing both the number of potential victims and the stealthiness of the attack.


B. DTV Service Characteristics

The study assumes a DTV service broadcasted by a main transmitter and a multiple frequency network (MFN) gap-filler. The main center transmits the DTV signal from an antenna at 100 m a.g.l. and an ERP of 62.6 dBm. A previous network planning exercise was carried out to ensure a signal level of approximately −70 dBm in locations close to the limit of the service area.

In the case of the gap-filler, the receiving subsystem uses an antenna of 11 dBd, at 15 m a.g.l. and a maximum output ERP of 42 dBm. The system accepts a signal input range from −77 dBm to −7 dBm (see Fig. 10).

![Gap-filler scheme](image)

Table VI describes the DVB-T modes considered in the simulations. These modes are displayed along with the corresponding threshold values. The link budget has been elaborated using the standard DTV network planning calculation procedure as shown in [28], [33].

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>64QAM</th>
<th>16QAM</th>
<th>QPSK</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Receiver Noise Figure (dB)</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Pn</td>
<td>Receiver Noise Input Power (dBW)</td>
<td>-128.16</td>
<td>-128.16</td>
<td>-128.16</td>
</tr>
<tr>
<td>Ps</td>
<td>Required C/N at Receiver Input (dB)</td>
<td>15.41</td>
<td>12.07</td>
<td>4.87</td>
</tr>
<tr>
<td>Ps min</td>
<td>Minimum Receiver Input Power (dBm)</td>
<td>-82.66</td>
<td>-85.46</td>
<td>-93.36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-91.06</td>
</tr>
</tbody>
</table>

Table VI: Link budgets

C. Attacker Infrastructure

The attacker uses a reception system in order to acquire the desired signal and modify the transport stream to be received by the Smart TV without suffering any perceptual change in the audiovisual content. In addition, the attacker uses a transmitting system that will be adapted to each one of the attack scenarios.

Table VII provides a summary of the reception and transmission parameters considered for simulating the attacks.

The geographical location of the attacker with respect to the victim population has also been analyzed in these simulations. Three different options were taken into account. The first option includes all the cases where the attacker is located at an equivalent height similar to the one of the rooftop antennas for DTV reception. In this case, the attack can be carried out using either a directive or omnidirectional antenna. A second option accounts for an attack carried out from a location at street level. In this case an omnidirectional antenna was considered.

D. Methodology

The potential success of an attack was studied using field strength maps calculated using the Longley Rice method [34], [35]. Table VIII contains the simulation data considered in this regard.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Longley Rice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td>700 MHz</td>
</tr>
<tr>
<td>Permittivity</td>
<td></td>
<td>4 (urban ground)</td>
</tr>
<tr>
<td>Climate</td>
<td></td>
<td>Temperate-continental</td>
</tr>
<tr>
<td>Location variability</td>
<td></td>
<td>95 %</td>
</tr>
<tr>
<td>Surface refractivity</td>
<td></td>
<td>301</td>
</tr>
<tr>
<td>Time variability</td>
<td></td>
<td>50 %</td>
</tr>
<tr>
<td>Conductivity</td>
<td></td>
<td>0.001 S/m (urban ground)</td>
</tr>
</tbody>
</table>

Table VIII: Field strength calculation parameters

The basic starting point to evaluate the potential attack was the field strength values of the desired signal over the area of study. In addition, three other parameters associated to the attacker’s signal levels were considered:

1) Attacker’s field strength level received at each location within the service area
2) Attacker’s interference ratio within the broadcaster’s coverage area
3) Broadcaster’s interference ratio within the attacker’s coverage area

A set of color maps obtained from the values calculated for each one of the previous parameters were processed using a software tool designed specifically for this study. This tool provides the percentages related to the correct reception of the broadcaster’s signal (green), the correct reception of the attacker’s signal (red), and the mush zone (black) for both, the area of the considered simulation maps and the area of interest for the study (see Fig. 11). Also, the software evaluates the percentages of locations associated to each scenario (green, red and black).

E. Case I Results: Attack against Fixed Reception Users

The case of an attack against a user that gets the desired service using a rooftop antenna assumes, for the sake of simplicity and efficiency of the attack, that the victim is located...
at the fringe of the coverage region. These users receive a desired signal close to $-70$ dBm and a rogue signal in the range of $-47$ dBm. Table IX summarizes the features of this scenario.

<table>
<thead>
<tr>
<th>Attacker at rooftop height</th>
<th>Attacker at street level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directive antenna</td>
<td>Omni antenna</td>
</tr>
<tr>
<td>Desired</td>
<td>99.8895%</td>
</tr>
<tr>
<td>Rogue</td>
<td>0.0006%</td>
</tr>
<tr>
<td>Mush zone</td>
<td>0.1099%</td>
</tr>
</tbody>
</table>

TABLE IX: Location percentage statistics of an attack to fixed receivers

The results show that the most critical case corresponds to the one where the rogue signal is transmitted with an omnidirectional antenna from a location slightly higher than the average rooftop height a.g.l. On the weak side for a potential attacker, the mush zone in this case is also the widest one. Nevertheless, the numbers do not provide significant differences between the three cases. In the worst scenario the ratio between the area where the attack is successful and the mush zone is $0.5\,\text{km} / 3\,\text{km}$.

The conditions for the attacker improve if a more robust mode is used (QPSK 2/3). In this case, the success area doubles and the mush zone remains stable ($3.4\%$ of the locations of the area of interest).

F. Case II Results: Attack against Portable Reception Users

The attack against portable reception users gives significantly worse results, from the attacker’s point of view. The number of victims decreases but at the same time the mush zone is also reduced. Table X shows the percentages calculated for the attack against portable users.

According to the values obtained in this case, this scenario could be chosen for an attack aiming at a specific group of receivers. The simulations show that the attacker at an equivalent rooftop height would be able to hack an area of $65 \times 65\,\text{m}^2$. The situation does not change significantly if the attack is carried out using a more robust mode.

G. Case III Results: Attack against a Gap-Filler

This scenario describes a situation where the number of potential victims is relatively large. The gap-filler is attacked by over powering the input signal with the rogue component, which, in consequence, will be re-broadcasted by the output power modules of the gap-filler over its service area. It was assumed that the attacker system location to send the rogue component using a directional antenna is at a distance of $30\,\text{m}$ away from the gap-filler site. In this case, a major problem to be solved by the attacker is the adjustment of appropriate input levels at the gap-filler receiving antenna, avoiding transmitter saturation. Table XI shows the signal values assumed by this simulation exercise.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{rav}$ - $P_{rbv}$</td>
<td>19.6 dB</td>
</tr>
</tbody>
</table>

TABLE XI: Signal levels at the gap-filler input

These values lead to conclude that the attack would be successful, since the rogue signal would be received $20\,\text{dB}$ over the desired service; a value high enough for correct reception of the mode 64 QAM 2/3. In this scenario, vulnerable Smart TVs within the gap-filler service area will be compromised.

Also, the rogue signal can interfere with the desired signal received by final users at the gap-filler input frequency ($f_1$ in Fig. 10). Table XII provides data associated to this case. These numbers show that the percentage of locations where this situation occurs is close to $9\%$ of the simulation area.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired coverage ($f_1$)</td>
<td>91.0293%</td>
</tr>
<tr>
<td>Rogue (received directly at $f_1$)</td>
<td>0.0005%</td>
</tr>
<tr>
<td>Mush zone</td>
<td>8.9702%</td>
</tr>
</tbody>
</table>

TABLE XII: Victim location percentages of interference (gap-filler)

H. Conclusions

The main conclusion of the simulated cases is that DTV consumers that use vulnerable Smart TVs can be attacked by using an infrastructure that is relatively simple. A second relevant conclusion is that the number of potential victims is
Fig. 12: The first two bars represent the DVB-T2 signals from the radio towers at Alexanderplatz and Schäferberg, respectively, and their respective echoes generated by the on-site on-channel gap-filler. The Alexanderplatz echo is the strongest signal with a margin of more than 20 dB.

Fig. 13: Exemplary approximation of attacker-controlled (red) and affected (gray) area (mush zone). Red and green markers correspond to measurement points with service controlled by the rogue or regular station, respectively; dark and light gray markers indicate mush zone, where the rogue or regular signal is stronger, respectively.

VII. FIELD MEASUREMENTS

Broadcasters might have an interest in determining potential attack ranges in practice. This would typically involve specific locations within an area serviced by existing regular broadcast or relay stations. We propose a method that can be used in existing SFNs, does not interrupt service, and only requires an add-on license to operate a low-power on-channel gap filler.

A. Methodology

A common method for analysis of an SFN is based on channel estimation data collected from the scattered and continuous pilots of a received DVB-T signal. The resulting transfer function of the broadcast channel can then be transformed to obtain the channel impulse response. Peaks represent the transmitters in the SFN and the delays between them correspond to the distance from the receiver, as depicted in Fig. 12.

An attack can be simulated by operating a gap filler that is synchronized to the SFN. Field measurements in the vicinity of the gap filler will then reveal the received power of each signal source via the channel impulse response. If the signal from the gap filler exceeds all other signals by the required amount of CCPR, this location would be part of the attacker-controlled area in a real attack. The attacker-affected area can be determined similarly (see Sect. V-B).

B. Field Trial

We performed a field trial in Berlin, Germany, to evaluate this method in practice. Two radio towers, located at Alexanderplatz and Schäferberg, provide the city with the recently launched DVB-T2 service. They operate as an SFN on channel 42, each with 50 kW ERP, using DVB-T2 variant G8 [29]. To improve the DVB-T2 signal coverage within the International Congress Centrum (ICC) building hosting the International Radio Exhibition (IFA) 2016, an additional repeater is operated for the duration of the exhibition. The repeater is fed with a signal received by a rooftop antenna facing Alexanderplatz, which is retransmitted on-channel with an output power of 300 mW inside a hall of the building. Figure 13 shows the location and orientation of the transmitting antenna (Kathrein 75010128).

A series of channel impulse response measurements were acquired in the vicinity of the repeater. Figure 12 shows one of these measurements: Each signal path is represented as a bar in a diagram, where the x- and y-axis indicate the delay and strength relative to the strongest signal, respectively. Here, the first signal to arrive originates from Alexanderplatz, followed by Schäferberg, and the respective echoes from the repeater; we are only interested in the Alexanderplatz signal and its

https://www.google.com/maps/@52.5025541,13.2706514,17z
echo. This data was acquired close to the repeater and therefore the repeater signal is much stronger than the original signal.

We then proceed to plot this measured difference in signal power on a map, for the entire measurement series. Depending on this value, locations are categorized as controlled by a potential attacker (red), mush zone (gray), or regular service (green). To qualify for the first or last category, the echo signal has to exceed or fall below the original signal by more than its CCPR, respectively; anything in between results in mush zone. The results of our field trial are presented in Figure 13.

VIII. CONCLUSION

This work demonstrates that DTV broadcasts can be abused to permanently and stealthily infect Smart TVs with malware, in less than ten seconds. It also reveals, however, that broadcast-based attacks are subject to serious limitations in terms of range and stealthiness. We thus revise previously published calculations regarding the size of an attacker-controlled area down by a factor of twenty, for a typical broadcast scenario. Furthermore, we show that such an attack creates a mush area without service coverage, which significantly aids broadcasters and authorities to detect and locate a commencing attack. Broadcasters should take appropriate measures especially to protect neuralgic points such as terrestrial gap fillers and cable TV headends. In the long term, broadcast standards should include mandatory authentication information, such that receivers can securely verify the origin and integrity of digital broadcasts.

ACKNOWLEDGMENT

The authors would like to thank Alexandra Mikityuk, Andrew Karpow, and the Hellmoltz Research School for Security Technologies for their help and support with this work.

REFERENCES


[19] ——, Digital Video Broadcasting (DVB); Subtitling systems (EN 300 743 V1.3.1), European Telecommunications Standards Institute, Jan. 2014.
[21] ETSI, Digital Video Broadcasting (DVB); Implementation guidelines for DVB terrestrial services; Transmission aspects (TR 101 190 V1.3.2), European Telecommunications Standards Institute, May 2011.
[24] ETSI, Digital Video Broadcasting (DVB); Signalling and carriage of interactive applications and services in Hybrid broadcast/broadband environments (TS 102 809 V1.2.1), European Telecommunications Standards Institute, Jul. 2013.
[26] ETSI, Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television (EN 300 744 V1.6.1), European Telecommunications Standards Institute, Jan. 2009.