A

Attacking the Internet using Broadcast Digital Television

Yossef Oren and Angelos D. Keromytis, Network Security Lab, Columbia University

In the attempt to bring modern broadband Internet features to traditional broadcast television, the Digital Video Broadcasting (DVB) consortium introduced a specification called Hybrid Broadcast-Broadband Television (HbbTV), which allows broadcast streams to include embedded HTML content which is rendered by the television. This system is already in very wide deployment in Europe, and has recently been adopted as part of the American digital television standard.

Our analyses of the specifications, and of real systems implementing them, show that the broadband and broadcast systems are combined insecurely. This enables a large-scale exploitation technique with a localized geographical footprint based on radio frequency (RF) injection, which requires a minimal budget and infrastructure and is remarkably difficult to detect.

In this paper, we present the attack methodology and a number of follow-on exploitation techniques that provide significant flexibility to attackers. Furthermore, we demonstrate that the technical complexity and required budget are low, making this attack practical and realistic, especially in areas with high population density – in a dense urban area, an attacker with a budget of about $450 can target more than 20,000 devices in a single attack. A unique aspect of this attack is that, in contrast to most Internet of Things/Cyber-Physical System threat scenarios where the attack comes from the data network side and affects the physical world, our attack uses the physical broadcast network to attack the data network.

Categories and Subject Descriptors: C.2.0 [**Computer-Communication Networks**]: General

General Terms: Design, Security, Experimentation

Additional Key Words and Phrases: Smart TV, radio-frequency attacks, relay attacks

1. INTRODUCTION

The battle for the living room is in full swing. After being used for decades as purely passive terminals, our television sets have become the subject of intense, competitive attention. Technology companies wish to use the Internet to create a viewing experience which is more engaging, interactive, and personalized, and in turn maximize their ad revenue by offering advertising content which is better targeted at the user. As the result of this trend, most US and European households with broadband Internet access now have at least one television set which is also connected to the Internet [The Diffusion Group 2013; Kamp 2013], either directly or through a set-top box or console. In technical terms, a device which has both a **broadcast** TV connection and a **broadband** Internet connection is called a **hybrid terminal**. The specification that defines how to create and interact with "hybrid content" (which combines both broadcast and broadband elements) is called **Hybrid Broadcast-Broadband Television**, or *HbbTV*.

Author's addresses: Yossef Oren and Angelos D. Keromytis, Computer Science Department, Fu Foundation School of Engineering and Applied Science, Columbia University in the City of New York, 1214 Amsterdam Avenue, New York, NY 10027, USA

DOI:http://dx.doi.org/10.1145/0000000.0000000

At its core, HbbTV combines broadcast streams with web technologies. The broadcast channel, augmented with the notion of separate digital streams, allows the transmission of distinct yet intertwined types of content that enable rich-interaction experience to the user. However, this enhanced interaction introduces new vulnerabilities to what was until now a conceptually simple network (TV broadcasting) and media-presentation device.

This paper examines the security impact of emergent properties at the intersection of digital video broadcasting and web technologies. The work presented here is based both on analysis of the HbbTV standard and on experimentation with actual DVB hardware. The attacks were crafted using low-cost hardware devices using open-source software, and they are extremely easy to replicate.

While the impact of many of these attacks is exacerbated by poor implementation choices, for most attacks the core of the problem lies with the overall architecture, as defined in the specification itself. Thus, our findings are significantly broader than the specific devices that we used in our analysis; indeed, *any* future device that follows these specifications will contain these same vulnerabilities. Exploiting these vulnerabilities, an attacker can cause many thousands of devices to interact with any website, even using any credentials stored in the TV sets for accessing services such as social networks, webmail, or even e-commerce sites. This capability can be leveraged to perform "traditional" attack activities: perform click-fraud, insert comment or voting spam, conduct reconnaissance (within each home network or against a remote target), launch local or remote denial of service attacks, and compromise other devices within the home network or even elsewhere. Beyond these, the attacker can also control the content displayed on the TV, to craft phishing and other social engineering attacks that would be extremely convincing, especially for TV viewers who are educated to (and have no reason not to) trust their screens. Finally, the attacker can use the broadcast medium to effectively distribute exploits that completely take over the TV set's hardware. Most of these attacks require no user knowledge or consent – the victims are only required to keep watching their televisions. The unique physical characteristics of the broadcast TV medium allow these attacks to be easily amplified to target tens of thousands of users, while remaining **completely undetectable**. Remarkably, the attacker does not even require a source IP address.

Today's smart TVs are already very complex devices which include multiple sensors such as cameras and microphones and store considerable amounts of personal data. Equipment manufacturers are busy adding more hardware and software capabilities to these devices, with the aim of turning them into the center of the user's digital life. Obviously, as smart TVs become more capable, and as users use them for more sensitive applications, the impact of the attacks described here will only grow.

One interesting, perhaps unique aspect of the problem space we are examining here is the reversal of attack source and destination domains: in typical attacks against Internet-connected physical systems, large-scale device compromise through the data network can lead to physical exploitation with a large (perhaps global) geographical footprint. With HbbTV, a physical attack with a relatively large geographical footprint can lead to large-scale data network compromise, at least in areas with high population density. The essence of the problem we address lies in that the hybrid TV now connects the broadcast domain, which has no authentication or protection infrastructure, to the broadband Internet domain. This allows the attacker to craft a set of attacks which uniquely do not **attack the TV** itself, but instead **attack through the TV**.

1.1. Disclosure and response

Our work addresses a security risk in a specification which is already in very wide use in Europe, and is on the verge of expanding to the US and to the rest of the world. We

thus made an effort to responsibly disclose our work to the relevant standards bodies. In December 2013, we provided a description of our RF-based attack, together with a video recording of an attack in progress, to the HbbTV Technical Group. In January 2014 we were informed that the HbbTV Technical Group discussed our disclosure, but did not consider the impact or severity of these attacks sufficient to merit changes to the standard. There were two main criticisms raised by the HbbTV Technical Group. The first criticism was that it would be very difficult for the attacker to reach a large number of systems; the second was that, even when an attack is carried out, a Smart TV has a very limited attack surface, so attacks would not be cost-effective. We explicitly structured this paper to address both of these criticisms – we quantitively demonstrate how a low cost attack can reach thousands of systems, and we show how attacks can cause a considerable amount of damage and provide a real financial gain for the attacker.

Document Structure: The rest of the document is arranged in the following manner: Section 2 provides a high-level overview of digital video broadcasting. In Section 3, we describe the fundamental weaknesses of the protocol which enable our attack and propose an attack setup designed to exploit them. Next, in Section 4 we describe a series of possible attacks based on these weaknesses. In Section 5 we discuss the radio-frequency aspects of our proposed attack. We continue with Section 6, where we quantitatively analyze the impact potential of our attack using a geoinformatic survey. In Section 7 we experimentally verify several of our proposed attacks. In Section 8 we analyze the financial impact our attacks and evaluate several possible countermeasures. Finally, we conclude in Section 9.

2. FUNDAMENTALS

The vision of an Internet-powered living room brings to mind products such as on-demand video streaming or cloud-delivered gaming. However, the masters of the living room are still the incumbent operators of existing television broadcast networks, who broadcast their content to billions of viewers worldwide. In order to compete with the new generation of entertainment content, the operators of these broadcast networks are also looking for ways to add Internet-based functionality to their traditional content. For example, a broadcast television channel might use Internet functionality to ask its viewers to participate in an online poll, or to vote for a candidate in a game show. The broadcast channel might also invite the viewer to learn more about an advertised product using interactive web content, or even replace regular broadcast advertisements with custom-delivered Internet ads personalized to the particular user. In this form of content delivery enhances traditional broadcast content with an interactive HTML overlay, rendered by the TV together with the normal broadcasted channel. This content is commonly called "**Red Button Content**", since pressing the red button on the TV remote is (by convention) the standard way of interacting with it.

The specification defining this behavior is called **Hybrid Broadcast-Broadband Television**, or HbbTV, and it is maintained by the European standards body ETSI [European Broadcasting Union 2012]. The current generation of the specification, version *1.2.1*, is enjoying very rapid adoption and is in active deployment or in advanced stages of testing in most of Europe. In December 2013, the Advanced Television Systems Committee (ATSC), which defines the digital video standards in the US, Canada, South Korea and several other countries, published a candidate standard for hybrid TV in America [Committee 2014]. This candidate standard shares much of its structure with the European HbbTV standard, and is specifically equivalent to the European standard with respect to the attacks described in this paper.

HbbTV is designed to work on top of a standard Digital Video Broadcasting (DVB) system. While DVB can be delivered over cable, satellite or standard terrestrial signal, each with its unique radio frequency (RF) modulation and transmission scheme, the underlying digital stream is essentially the same for all delivery methods. This stream takes the form of an MPEG-2 **Transport Stream** [International Standards Institute 2013], which multiplexes together multiple data streams named MPEG-2 **Elementary Streams**. Each elementary stream carries an individual element of a television channel, such as video, audio or subtitles. Special **metadata streams,** which the specification refers to as **information tables,** are then used to group together multiple elementary streams into an individual TV channel and provide additional information about the channel such as its name, its language and the list of current and upcoming programs. A single radio physical frequency may thus carry multiple channels.

2.1. Mixing broadcast and broadband

The HbbTV specification extends standard DVB by introducing additional metadata formats which mix broadband Internet content into the digital television channel. While the specification proposes multiple ways in which web content can be used in a TV, this article will focus on the most common form of content, **autostart broadcast-dependent applications**. This form of content starts running automatically when the user tunes into a particular TV channel, and terminates when the user moves to another channel. To create an autostart broadcast-dependent application, the broadcaster includes in the MPEG transport stream an additional **application information table** (AIT) describing the broadband-based application, then references this table in the **program mapping table** (PMT) describing a certain TV channel. The HbbTV specification defines two possible ways of providing the application's actual web content (*i.e.,* HTML pages, images, and scripts). One way is to have the AIT include a URL that points to a web server hosting the application. Another possible way is to create an additional data stream which includes the HbbTV application's HTML files, deliver this additional elementary stream over the broadcast transport, and finally have the AIT point to this data stream. The way in which the latter embedding method was realized leads to a serious security problem, as we discuss later.

Regardless of the delivery method, Internet content is rendered by the TV using a specially-enhanced web runtime, described in the HbbTV standard as a Data Execution Environment (DAE) [Forum 2012]. In addition to the document object model (DOM) elements available to normal HTML environments such as XmlHttpRequest, the DAE exposes additional DOM elements which are specific to the television world (for example, information about the running program and the current channel). The DAE also allows programatic access to the live TV broadcast window. Thus, it is possible for an HbbTV application to render content on top of the TV broadcast, resize the broadcast window or even completely replace the broadcasted content with its own content. On the other extreme, it is also possible for an HbbTV application to run without displaying any indication to the user. Practically speaking, most "benign" applications typically display a small overlay inviting the user to press the Red Button, then disappear to run transparently in the background.

2.2. Security in HbbTV

Smart TVs are built with some consideration of security, since they are often used to display content protected by digital rights management (DRM) schemes. Indeed, the HbbTV specification dedicates an entire chapter to security, but the discussion is mainly focused on protecting DRM content and not on other aspects of security. To that effect, the HbbTV specification describes trusted and untrusted applications, and restricts "sensitive functions of the terminal" only to trusted applications. Examples

of such "sensitive functions" include downloading and playing back DRM-protected downloaded content (actions which may incur a cost on the viewer), as well as configuring and activating the terminal's scheduled recording (time-shifting) capabilities.

The attacks described in this work make use of capabilities which are available both to trusted and untrusted applications. None of the attacks described in this work are restricted in any way by HbbTV's security mechanisms. Furthermore, since the specification does not strictly define how an application can become trusted, it might be possible to inject an attack into a trusted application without changing its trusted status.

3. ATTACK CHARACTERIZATION

Several unique properties of HbbTV make it potentially prone to attack. These security weaknesses can all be considered **emergent** properties, which exist on the boundary between the broadband and broadcast systems, and stem from the different expectations and guarantees which exist in each system.

First and foremost, HbbTV applies a very problematic security model to web content embedded into the broadcast data stream. This is, in our opinion, the most serious security flaw in HbbTV, and one which has not been discussed in any previous work. One of the cornerstones of modern web security is the Same-Origin Policy [Barth 2011], which essentially serves to isolate content retrieved from different origins and prevent content from one web site from interfering with the operation of another web site. Under the same origin policy, each piece of web content is provided with an origin consisting of a tuple of scheme, host and port, and two resources are limited in their communications unless they share the same origin.

When an HbbTV application is downloaded from the Internet via URL, the origin of the web content is clearly defined by the URL, appropriately isolating HbbTV applications to their own domain and preventing them from interfering with Internet at large. However, when the content is embedded in the broadcast data stream it is not linked to any web server and, as such, has no implicitly defined origin. The HbbTV specification suggests [European Broadcasting Union 2012, S 6.3] that in this case the broadcast stream should **explicitly define its own web origin** by setting the `simple_application_boundary_descriptor` property in the AIT to any desired domain name.

The security implications of this design decision are staggering. Allowing the broadcast provider control over the purported origin of the embedded web content effectively lets a malicious broadcaster inject **any script of his choice** into **any website of his choice**. It should be noted that the HbbTV specification explicitly allows both HTTP and HTTPS schemes to be defined as the web origin for broadcast-delivered content. Thus, scripts can also be injected into secure websites such as webmail services.

An illustrative example of an attack exploiting this mechanism is presented in Figure 1. In this attack, which we discuss more extensively in Subsection 4.2, the adversary delivers a malicious Javascript payload over HbbTV, and furthermore indicates by the `simple_application_boundary_descriptor` property in the AIT that this payload's web origin is a rating site. Next, the attacker has the TV render a simple HTML page which embeds the real rating site's home page (downloaded from the broadband Internet), as well as this script, in a zero-sized frame. The malicious script now has full programmatic access to the content delivered by the rating site, since it is running within the same web origin. To make matters worse, if the user has previously logged on to the site, this attack allows the attacker to fully interact with the website on the user's behalf. While the innocent viewers enjoy their normal television content, the malicious application causes their infected TVs to interact with the rating site over

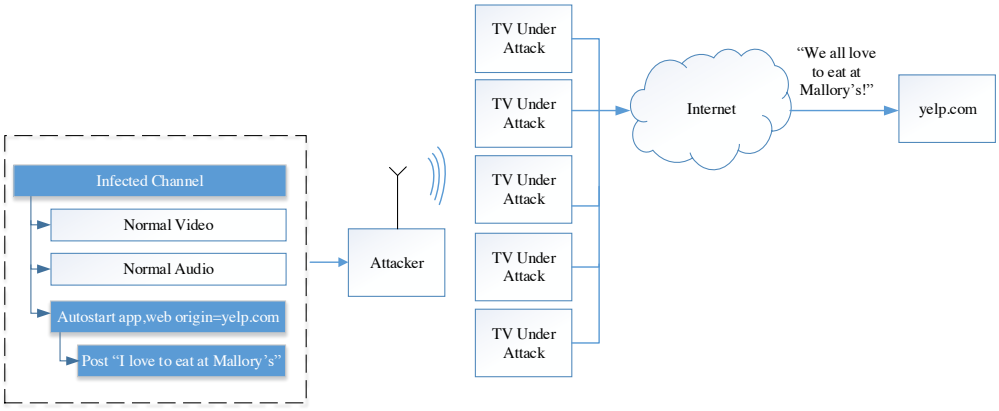


Fig. 1: A practical attack based on a malicious HbbTV application. In this attack the malicious player forces multiple infected TVs to interact with a rating site and leave a favorable review for his restaurant.

the Internet to leave favorable reviews for the attacker's restaurant or to harass his competitors.

3.1. General Principle of Operation

We now describe how an attacker can use the vulnerability described above to launch a series of large-scale attacks. Our setup targets digital terrestrial television (DTT), which is the most common way in which television is received in many parts of the world [European Commision 2013]. In Subsection 8.2 we discuss how this attack can also be applied to other delivery methods such as cable or satellite.

Our attack works by creating a television broadcast which includes, together with the normal audio and video streams, a malicious HbbTV application. To maximize the effectiveness of our attack, we would like this as many users as possible to tune into this broadcast. The best way to do so is to carry out a form of **man-in-the-middle attack**, in which the attacker transparently modifies a popular TV channel to include a malicious payload.

Our attack module follows the general design illustrated in Figure 2. Following the notation of Subsection 2.1, the attacker adds into the intercepted stream a new **Application Information Table**, as well as a **data stream containing a malicious HbbTV application**, which the new AIT points to. The attacker then modifies one or more existing **Program Mapping Tables** to reference the new malicious application, while leaving the audio and video contents of the channel unmodified. It is important to note that the attacker does not have any form of control or cooperation with the radio tower itself.

The physical attack setup required by the attacker is illustrated in Figure 3. The attacker's uses a **receive antenna** connected to a **DVB tuner** to intercept a legitimate television signal, **modifies the content** of the DVB stream to add its malicious payload, and finally uses a **DVB modulator** connected through a **power amplifier** to a **transmit antenna** to re-transmit the modified signal to the **TV under attack** using the same frequency as the original broadcast. The TV under attack is, in turn, connected to the Internet.

Our attack works because in a certain geographic area around the attacker the malicious modified signal will be stronger than the original signal transmitted by the tower. This will cause any televisions in the area to immediately fall victim to the at-

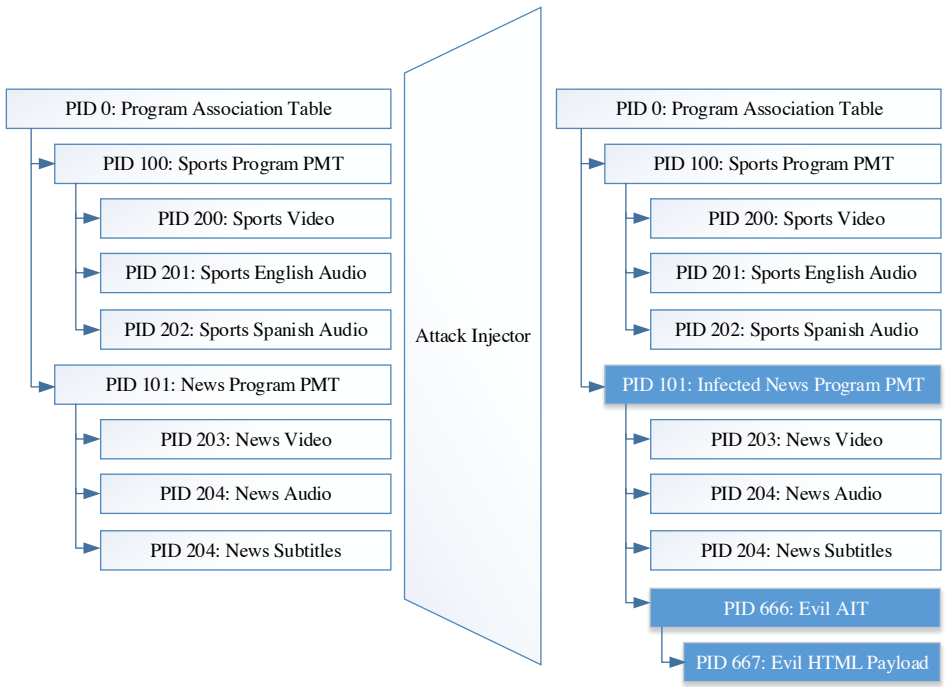


Fig. 2: Injecting a malicious application into a DVB stream. Note that only the program mapping table is modified, while the audio and video content is left untouched.

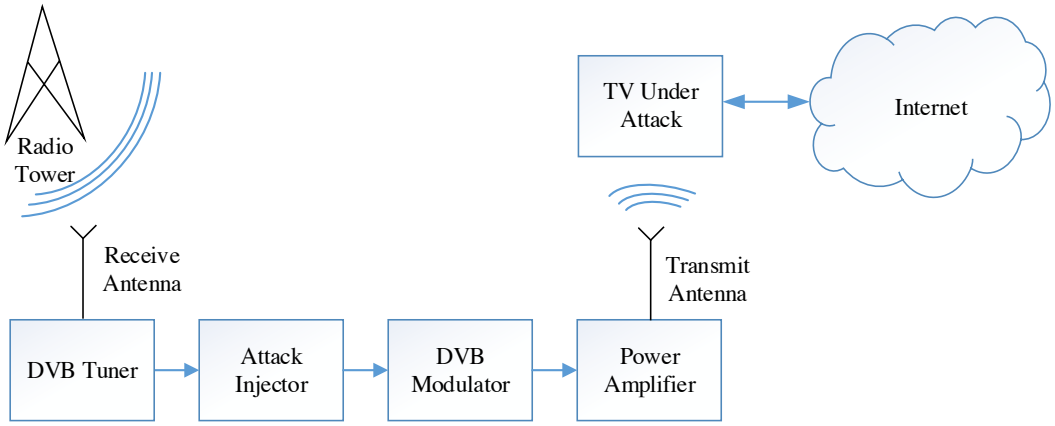


Fig. 3: Attack Setup

tacks described below. We note that since in digital broadcasting multiple TV channels are sent from the radio tower using the same radio frequency, a single attack setup is capable of injecting attack code into several channels simultaneously.

The characteristics and estimated cost of each of the components in Figure 3 are presented below:

Receive antenna and DVB tuner – a USB-powered DVB tuner and a short passive antenna can be purchased online for about $15. The open-source VLC media

player [Organization 2014] is capable of interfacing with many of these tuners and sending the demodulated stream extracted from an entire RF channel to a file or a network socket.

Content modification – the demodulated stream is modified to contain a malicious application (either as a URL, or as a full application delivered via data stream), and the PMTs of all TV channels in the demodulated stream are modified to auto-start this application as soon as the user tunes into the channel. Since the video and audio streams in the channel are forwarded without any modification, this operation is not particularly computation intensive, and any low-cost computer with USB 2.0 support can be used for this purpose. A software suite named Avalpa OpenCaster [Engineering 2014] provides a set of open-source command-line tools which can be used to modify a multiplexed DVB stream in real time.

DVB modulator – this hardware component takes a multiplexed MPEG stream and converts it into an RF signal suitable for transmission. While these devices were once massive and expensive, modern DVB modulators are remarkably small and easy to use – a full-featured USB-powered modulator which can interface with OpenCaster can be purchased online for less than $200.

Power amplifier and transmit antenna – the attacker needs to create a signal that is stronger than the original TV tower's signal and transmit it toward the target televisions. An attacker with a higher transmit power can affect more television sets, but a high-power setup is generally less portable, giving the attacker a higher probability of being detected and arrested. In Section 5 we formally analyze the power requirements of the attacker and show that, under the right conditions, a remarkably high amount of television sets can be affected with a moderate-to-low powered amplifier.

3.2. Additional Security Weaknesses

3.2.1. Attacks are untraceable. In traditional Internet-borne attacks, it is always assumed that the attacker is himself present on the Internet before he can deliver a malicious payload to his victims. The attacker's IP and DNS entries can then be used by intrusion protection services and law enforcement agencies to protect against the attack as it occurs, and to trace and prosecute its perpetrators after it has concluded. In contrast, our attacker needs no such infrastructure to deliver its malicious payload. It is surprisingly simple and inexpensive to build a digital terrestrial television (DTT) transmitter and use it to reach thousands of potential hosts. After the attack concludes, the attacker leaves no trace of his activities in the form of IP or DNS transactions.

Operating an unlicensed TV transmitter is illegal in many countries. Law enforcement agencies capture these illegal transmitters by **triangulation** methods, which involve sending multiple car-mounted receivers to the vicinity of the attack, then using the differences in received signal strengths between receivers to locate the rogue transmitter. A sensitive receiver can also "fingerprint" the rogue transmitter's RF envelope and help recognize it in the future. While this defense mechanism can potentially trace our radio attacker, mobile triangulation is a **reactive** defense step, which requires a considerable expense of time and resources from the defender's side. Considering that the attack we describe has a very limited geographical signature, operates for a very limited time (potentially only a few minutes), and causes no visible adverse effects to the user, it is highly unlikely that the attacker will be caught by these methods.

3.2.2. Attacks are invisible and unstoppable. HbbTV content is not required by standard or convention to offer any visual indication that it is running. Depending on the choice of the application creator, HbbTV content can run invisibly in the background, side by side with the broadcast content, or even take over part or all the user's entire screen.

At one extreme, this makes it possible for HbbTV applications to run completely in the background without the knowledge or consent of the user. In [Herfurt 2013b] Herfurt discovered that many German broadcasters are using this functionality of HbbTV to invisibly track the viewing habits of users by periodically "phoning home" while the TV is tuned to a particular channel. At the other extreme, it is possible for an HbbTV application to take over part or all of the user's screen without his knowledge. Herfurt used this functionality to demonstrate a proof-of-concept application that replaces the news ticker of a German news channel with headlines from a satire website.

Another related weakness is the weak control the user has over the life-cycle of HbbTV applications. As described in Subsection 2.1, an application can start running automatically as soon as the user starts viewing a certain channel. More troubling is the fact that, once an HbbTV application has started running, there is no standard way of **stopping** it, short of switching a channel, turning off the television, or completely disabling HbbTV support.

4. ATTACKS

The attacks proposed in this Section are based upon our analysis of the HbbTV standards, as well as upon personal communications with the HbbTV technical group, who have confirmed that our attacks are possible given the current specification. Some of these attacks described below can be applied even to perfectly secure Smart TV implementations with no known exploits; Other attacks allow the attacker to transform local vulnerabilities on the Smart TV into automatic, large-scale distributed exploits. With the exception of the attack described in Subsection 4.5, all of these attacks take place without the user's knowledge or consent, requiring the user to do nothing more than keep his TV turned on and tuned to his favourite channel.

4.1. Distributed Denial of Service

To carry out this attack, the attacker creates a simple Red Button application which repeatedly accesses a target website with high frequency, using a simple mechanism such as a zero-sized `iframe` element or through repetitive calls to `XmlHttpRequest`. All TVs tuned to the infected channel will immediately start running the application, potentially overwhelming the target website. Due to the design of the HbbTV specification, the owners of TVs who are carrying out this attack have no knowledge that they are participating in this attack, nor do they have any way of stopping it.

This attack is the simplest abuse of the HbbTV protocol, and was also considered by [Herfurt 2013b], albeit in a different attacker model. As scary as this attack sounds, we note in Subsection 8.1 that there are far less expensive and risky ways of DDoSing a website.

4.2. Unauthenticated Request Forgery

This attack is similar to the previous attack, but this time the infected users do not blindly access the site under attack, but instead attempt to interact with it in a meaningful manner. For example, such an attack could skew the results of an online poll or competition, "spam" a forum with comments to the point of unreadability, falsely promote another website by "liking" or "up-voting" it, or falsely obtain ad revenue by programmatically clicking on an ad (a.k.a. "click fraud"). This attack venue is especially painful for the designers of HbbTV, since the entire point of the specification is to allow this type of interaction between TV viewers and websites.

This attack is a variant of traditional cross-site request forgery (CSRF) attacks, which are well-known to the security community [Barth et al. 2008]. However, one unique advantage of the HbbTV attack vector is that the attack is not "blind" – due to the unique way same-origin is implemented for HbbTV, the attack script can fully

interact with the static and dynamic content of the page with the full permissions of a human user accessing the webpage. This defeats many of the state-of-the-art defenses against CSRF, which operate by embedding session and authentication tokens in locations which are only accessible within the same origin as the protected web page.

This attack can be compared to "universal cross-side scripting" (UXSS) attacks, which similarly allow arbitrary attacker-controlled scripts to be run on arbitrary web pages. Previously disclosed UXSS attacks typically leveraged vulnerabilities in web browsers or in common plugins, and required that the victim click on an attacker-controlled link or browse to an attacker-controlled website [Shezaf 2007; National Vulnerability Database 2011]. The attack described here is unique in being a network-level attack, which requires no action on the side of the victim.

4.3. Authenticated Request Forgery

An interesting twist on the previous attack, this attack assumes that the user has previously authenticated to a certain website using another application on his Smart TV, and that the TV now holds a cookie, an HTML5 local storage element, or any other authentication token for this website[1]. When the infected application accesses the website, it will now automatically do so with the full credentials of the logged-in user, a fact which dramatically increases the damage potential of the previous attack. An infected application using this attack vector can, for example, post links to malware to the legitimate user's friends over Twitter or Facebook, purchase DRM-protected content whose royalties are pocketed by the attacker, or call a premium number using a VoIP application. As the usage scenarios of Smart TVs grow and users begin using them for more applications such as e-commerce and health, the damage potential of this attack will grow rapidly.

4.4. Intranet Request Forgery

This attack makes use of the fact that the Smart TV is most likely connected to a home wireless network shared with other devices such as wireless routers, personal computers and printers. Instead of attacking the whole Internet, the attacker instead mounts his attacks on those local intranet devices. The most basic attack would be a port scan to discover which devices are present on the home network (this can assist in planning a burglary). If vulnerable devices are discovered on the network, the attacker can also try and exploit them using the Smart TV. For example, the attacker can identify a vulnerable wireless router and a Windows PC, then proceed to modify the DNS settings of the router so that the PC is directed to a phishing website when it attempts to connect to a banking website. This attack, which again has been investigated in other works such as [Johns and Winter 2007], is particularly effective due to the way same-origin is implemented on HbbTV. Remarkably, the attacker's code can freely interact with the device under attack and observe the results of its interaction, without requiring additional steps such as DNS rebinding.

4.5. Phishing/Social Engineering

As described in Subsection 3.2.2, HbbTV content is displayed on the user's television without any warning or notification, and the user cannot turn it off without turning off

[1]It should be noted that by default, Android and iOS smart phone applications provide an isolated location for credential storage for each application, including the built-in web browser. While the smart TV platform we evaluated was not built on top of Android or iOS, it also had two separate "web runtimes" – one for the TV's built-in browser and one for the HbbTV stack – and thus kept credentials isolated. We suspect that this behavior was caused by engineering concerns (two independent teams may have written the two runtimes, with no time for integration). Credential isolation is in no way required by the HbbTV standard.

the TV itself. HbbTV content can completely overlay the user's TV broadcast and can programmatically interact with many of the buttons on the user's remote control. This direction, also investigated by Herfurt in [Herfurt 2013b], makes HbbTV content a natural vector for attacks which mislead the user into divulging sensitive information or otherwise acting in a harmful manner.

For example, a malicious HbbTV payload can notify the user that he must enter his credit card information to view some restricted content, compel the user to change the configuration of their network in a form that compromises their security (for example, instruct the user to press the WPS button on their wireless router, thus allowing a malicious device to join the network), or even encourage "real world" risky behavior, such as notifying the user that a "cable technician" is due to visit their house at a certain time and date, or that the TV needs to be "recalled" and physically delivered to the attacker. This attack is different than the other attacks described in this paper since it requires user interaction and, as such, is more likely to be detected or simply ignored. Obviously, the damage potential of this attack will increase in the future as more users are trained to interact with their TVs for applications other than passive content consumption.

4.6. Exploit Distribution

A modern smart TV is essentially a personal computer with a very limited user interface, running a highly modified version of Linux or Android. Just like normal PCs, security exploits are occasionally discovered in Smart TVs – either in the vendor's proprietary software, or in the device's various open-source underlying components. Just like normal PCs, Smart TVs also have automatic software update mechanisms which are generally successful in keeping the TVs running smoothly and securely. However, the vulnerability-to-patch cycle for these devices is typically much longer than that of a desktop operating system, due to the additional steps required by the equipment vendor to implement, test and deploy security updates for this nonstandard platform. Whenever an exploit is discovered for a Smart TV platform, the combination of HbbTV's invisibility and undetectability make it a remarkably efficient method of distributing this exploit and compromising the TVs.

Assume, for example, that a Smart TV uses an open-source image processing library as part of its code. Assume now that a patch is released to fix a vulnerability in the upstream version of this component. While the equipment vendor is busy porting, testing and deploying a patch specifically tailored for the smart TV, an attacker can immediately craft an exploit corresponding to this vulnerability, embed it in a malicious Red Button application, then immediately deploy it to thousands of Smart TVs.

5. RADIO-FREQUENCY ASPECTS

In this section we discuss the radio-frequency aspects of our proposed attack. We define the physical characteristics and limitations of the attack, and suggest a working point for the attacker which balances efficiency and cost. This section analyses attacks on digital terrestrial television (DTT). In Subsection 8.2 we discuss how variations on this attack may also be applied to other distribution methods, such as satellite or cable. For efficiency of discussion, we make several simplifying assumptions in this section. Subsection 5.3 lists these simplifications and explains their impact on the actual effectiveness of our proposed attack.

5.1. Signal propagation fundamentals

Our proposed attack requires the attacker to set up a rogue TV transmitter which overwhelms a known TV station's signal in a limited physical area. The attacker's signal is broadcast on the original channel's frequency and contains the original channel's audio

and video content. The attacker's signal also contains a malicious payload in the form of an HbbTV application. Within the limited area of attack, all victim TV sets which were originally tuned into the original station will instead receive the attacker's signal and automatically participate in the attack. For the attack to succeed we thus require that the following three conditions must hold:

(1) There exists a sufficient amount of Internet-connected TV sets in a certain geographical area
(2) There is a popular TV station whose broadcast signal can be received by these TV sets
(3) The attacker's setup allows him to overwhelm the TV station's original broadcast signal in this area and substitute it with his own malicious signal

There are therefore three parties whose interaction creates an effective attack – the victim TVs, the TV station, and the attacker.

We can obtain the approximate amount of TV sets in a certain area by extrapolating from publicly available population density measurements. We note that according to [The Nielsen Company 2014] the relation between population count and TV count in the United States is approximately 0.3 TV sets per person.

There are several parameters which determine how a TV station's signal propagates from the TV station's broadcast tower to the TV set. The most significant parameters are the TV station's transmit power, and the distance between the TV broadcast tower and the TV set. The transmit power is typically measured in dBm, a logarithmic unit of measurement in which 0 dBm stands for 1 milliwatts. A full-strength TV tower can have a effective radiated power P_S of up to 75 dBm. Another parameter is the frequency f of the radio transmission. Digital TV stations operate either in the VHF or UHF frequency bands. The calculations in this section use a representative frequency of 500MHz, corresponding to a TV station in the UHF frequency band.

As the radio-frequency signal propagates through free space, its power decays exponentially. The decay in decibels of a radio signal with frequency f (in Hz) over a distance d (in meters) is described by the Free Space Path Loss equation [League 2013]:

$$FSPL(d, f) = 20 \log_{10}(d) + 20 \log_{10}(f) - 147.55$$

The strength of the signal incident upon the TV set's receive antenna is thus $P_S - FSPL(d, f)$. This signal is ultimately picked up by the TV set's receive antenna, together with a certain amount of noise. If the received signal's power is sufficiently more than the received noise, the signal may be decoded by the TV and finally displayed to the user. If the attacker's malicious signal, as it is picked up by the TV's antenna, is sufficiently stronger than the broadcast station's original signal, then the TV set will receive the malicious signal and display it instead.

5.2. Working Point Selection

For an optimal attack the adversary must choose an attack location which accommodates the interplay between the TV station, the victim TV and his own attack setup. If the original TV station is received with an overly high signal strength in the victim's location, the attacker will have to use an impractically powerful transmitter to overwhelm it and thus carry out his attack. If, on the other hand, if the original signal is too weak in the victim's location, it is unlikely that any of the victims' TV sets would be tuned to the channel, limiting the effectiveness of the attack. The attacker must also choose his transmit power carefully. Obviously, the attacker's transmit power must be high enough to overcome the legitimate station's original signal. However, the attacker also has incentives to keep his transmit power as low as possible. This is due to the fact that a higher-powered receiver typically has a higher cost, larger dimensions and

a higher power consumption, making the attack less cost-effective, less portable and easier to detect.

Let us now define the TV station's transmit power as P_S, the attacker's transmit power as P_A, the distance between the TV station and the victim as d_{SV} and the distance between the attacker and the victim as d_{AV}. For a successful attack would we would like the attacker's signal to overwhelm the original station's power, as they are both received at the victim's location: $P_A - FSPL\left(d_{AV}, f\right) > P_S - FSPL\left(d_{SV}, f\right)$.

If the attack area is small enough and distant enough from the TV tower, we can assume that the TV station's signal strength in the area of attack is constant. We denote this value by P_{SV}. The simplified requirement for the attacker is now:

$$P_A - FSPL\left(d_{AV}, f\right) > P_{SV}$$

Assigning into the FSPL equation, assuming $f = 500$ MHz and simplifying for d_{AV}, we arrive at:

$$d_{AV} < 10^{\frac{P_A}{20} - \frac{P_{SV}}{20} - 1.32}$$

The total area of attack is then the area of a circle with radius d_{AV}:

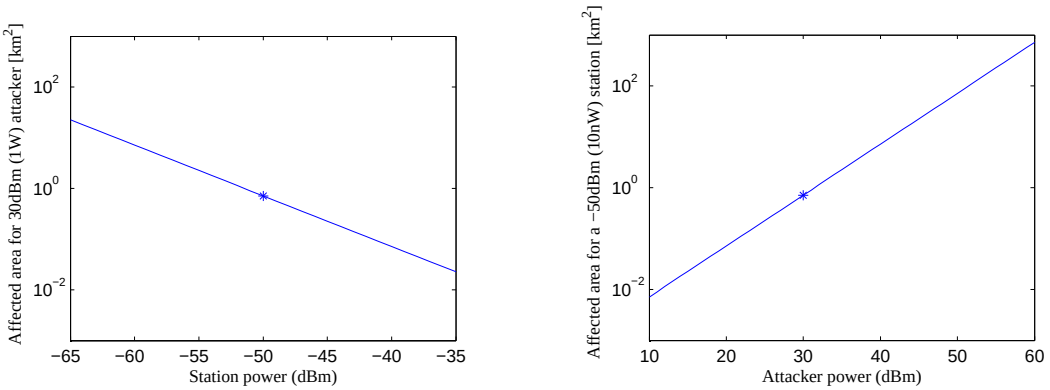
$$A = \pi d_{AV}^2$$

Let us now propose a possible working point which provides the attacker both with a reasonable attack area and with a reasonable transmit power. For the received signal level of the station under attack we chose P_{SV} = -50 dBm. This power level is reasonably higher than the minimum "city-grade" signal level of -61 dBm, which is considered strong enough by the FCC to be received with an unamplified set-top antenna [Commission 2001]. Assuming a TV station transmits a 75 dBm signal into a completely unobstructed area, this signal strength will be achieved for points between 75 and 95 km away from the TV tower. For the attacker's transmitter power, we choose $P_A = 30$ dBm, or 1W. Commercially available 1W power amplifiers operating in this frequency range cost less than $250, are passively cooled using a heat sink, and can be operated using a portable 12V battery. An example of such an amplifier is the Mini-Circuits ZHL-2010+ [Mini-Circuits 2010].

Figure 4 shows the effective area of attack with different attacker and station power levels, with the -50dBm (station) and 30dBm (attacker) working points indicated with a star. The effective area of attack for an attacker with a 30 dBm transmitter operating in an area with a TV signal of P_{SV} =-50 dBm is A =0.71 km^2.

5.3. Simplifying assumptions

Several additional factors must be considered before the attack described in this section can be made practical. The first factor is the shape of the transmit and receive antennas. TV transmission antennas are typically isotropic antennas, which radiate the same power in all directions. On the other hand, receive antennas, especially rooftop-mounted ones, are often directional antennas which are more sensitive to signals received from certain directions. An attacker attempting to overwhelm a TV tower's signal as it is incident on a directional receive antenna would have the best performance if his own transmit antenna is properly situated with respect to the TV set, optimally somewhere along the straight line connecting the two antennas. In an urban setting this condition can be realized if the attack is carried out from the roof of an appropriately located tall building. To reduce the attacker's risk of capture and thus increase the effectiveness of the attack, the attacker can also install the relay equipment on a remote controlled-drone and fly it to an appropriate location, similar to the work of [Reed et al. 2011].



(a) Attacker power fixed at 30dBm, variable station power

(b) Station power fixed at -50dBm, variable attacker power

Fig. 4: Effective attack areas for different attacker and station power levels.

A practical setup should also consider the attenuation factors due to the interfacing of the transmitter and receiver hardware and their respective antennas, as well as the directional gain factor of the antennas relative to an isotropic source. Both of these factors can slightly affect the effective radius of the attack d_{AV}, but their overall impact is minimal for most practical setups.

The attacker would also need to prevent his receive antenna from picking up his own signal. This can be achieved by splitting the attack setup into separate receiver and transmitter setups. The receiver setup will use a directional antenna directed toward the radio tower, while the transmitter setup will use a directional antenna directed toward the TVs under attack. Finally, the receiver setup should be located in one of the transmitter setup's "dead zones". The attacker can also use some physical obstacle (such as a building or a mountain) to separate the receiver and transmitter parts of the relay setup. Using a directional antenna setup as described will change the shape, but not the general area, of the location under attack.

Another factor is the issue of multi-path propagation and fading. In practical situations, the signal incident from the TV tower's transmit antenna may not travel directly to the receive antenna, but instead can be reflected from other buildings or terrain features before it being received. This can cause the actual signal strength at certain locations to be different than the one expected in a free space model. It should be noted that the attacker's signal is also subject to the same effect.

The final issue which needs to be considered is that of co-channel rejection. In our analysis, the TV set simply decoded the stronger of the two competing signals (either the original TV tower's broadcast or the attacker's malicious broadcast). In practical systems, if the difference in signal levels between the two stations is below a certain threshold the TV's decoding process will fail resulting in reception errors. This threshold is called the co-channel rejection margin, and its actual value depends on the exact modulation scheme chosen for a particular channel. In its formal specifications, the International Telecommunications Union recommends a rejection margin of 6 to 8 dB between the stronger station and the interfering weaker station [International Telecommunication Union 2014, Table 15]. There are, however, practical ways of reducing this rejection margin in practical cases. Specifically, the ATSC specification allows transmit towers to vary their pilot frequencies by a few KHz, allowing the receiver

to better tune on the stronger signal and reject the weaker one [Advanced Television Systems Committee 2008, §5.1.6.1].

6. GEOINFORMATIC SURVEY

In the previous section, we concluded that an attacker can carry out a reasonably effective attack using a 1W transmitter in an area where the TV station under attack is received with a signal strength of around -50 dBm. Having chosen a working point for the attacker, our next goal is to show that there exist densely populated locations where popular TV stations are received with the required signal strength. This section presents a geoinformatic investigation of our attack's effectiveness in practice, based on actual data about signal strengths and population densities in the continental United States. Our survey, which extends our initial report given at [Oren and Keromytis 2014], identifies thousands of locations where an attack will be particularly effective.

6.1. Data Sources and Methodology

We carried out our assessment step using geoinformatic databases describing both the population density and the received signal strengths of TV stations throughout the US. The population density information was drawn from the NASA Socioeconomic Data and Applications Center (SEDAC) data set [Seirup and Yetman 2006]. The SEDAC dataset in based in turn on census block geography from the 2000 U.S. Census. SEDAC produces two data sets describing population densities in the United States – a low-resolution data set covering the entire area of the U.S. and Puerto Rico, and a high-resolution data set covering 50 metropolitan areas with at least one million in population. The spatial resolutions of these data sets are approximately 1 km^2 and 0.04 km^2 per sample point, respectively. We used the high resolution data set in our analysis.

The TV signal strength information was extracted from a dataset made available by the website TVFool.com. This data set describes the received signal strength in the area around each of the FCC-licensed digital TV broadcasters in the U.S, assuming an isotropic receive antenna located 10 feet above ground level. The signal strength for each location is derived using 3D propagation modeling algorithms which consider transmitter power, terrain obstructions and the curvature of the Earth. The spatial resolution of the TVFool data set is approximately 0.025 km^2 per sample point. The TVFool.com website also offers the ability to calculate the precise signal strength of all nearby TV stations for any precise set of coordinates.

We analyzed and combined these two data set using the Matlab mapping toolbox and the open-source geographic information system QGIS [QGIS Project 2014].

6.2. Case Study: the Big Five in the Big Five

Most of the English-language TV viewership in the United States is claimed by five broadcast networks. These five networks (ABC, CBS, NBC, Fox and CW) each own a large quantity of local broadcast stations, and each individually claim to be viewable by at least 97% of the U.S. population. We investigate the susceptibility of each of these five networks to the attacks described in this paper, focussing on the five largest combined metropolitan status areas (CMSAs) in the US. The big five CMSAs are listed in Table I, together with the call signs for each one of the major broadcast networks in each of the areas. The additional call signs noted in parentheses indicate stations from the same broadcast network but belonging to neighboring markets. For example, Washington DC subscribers can also pick up TV broadcasts from Baltimore, while San Jose subscribers can pick up signals from Santa Cruz and from Modesto.

Figure 5 shows the effectiveness of our attacks in each of the five major CMSAs. Shaded areas in the map indicated areas in which the received power level of at least

one station makes it susceptible to attack (darker areas indicate more than one station). Stars indicate vulnerable areas where the population density is at least 10,000 persons per km^2. Table II shows the percentage of the area and of the population of each CMSA which is vulnerable to attack. To designate an area as vulnerable, the strongest signal corresponding to all TV stations in a certain network (including TV stations from neighboring markets) had to be in the range of -61 to -50 dBm.

Table III presents specific points in the surveyed CMSAs which are especially vulnerable to attack. These locations are characterized either by an extremely high population density, or by an abundance of TV stations which are vulnerable to attack. The list of stations included in this analysis also includes PBS and the popular Spanish language networks Telemundo and Univision. The coordinates given in Table III are approximates – we will make the exact coordinates available to researchers upon request.

As shown by the maps and figures, a remarkably large proportion of the landmass and populations of all surveyed areas was vulnerable to attack. This fact, combined with the low cost and high effectiveness of the proposed attack, leads us to believe that it is likely to be exploited in practice.

7. EXPERIMENTAL VALIDATION

To show the validity of our claims, we created a test setup and experimentally reproduced a few of the attacks proposed in this paper. Our attacks were carried out on a modern Smart TV, manufactured in 2012 and running the latest software version supplied by the vendor. Our DVB demodulator was an OEM DVB-T stick based around the highly popular Afatech AF9015 chipset. The broadcast DVB stream was captured using VLC Player [Organization 2014] running on Linux. Our DVB modulator was a DekTec DTU-215 unit, which was connected via USB to a low-cost laptop computer running Linux. For safety reasons our test setup did not include a power amplifier and transmitter antenna – instead, the DVB modulator was directly connected to the TV's antenna input through a 10 dB RF attenuator. The signal sent to the TV included different malicious HbbTV payloads created using the open-source OpenCaster package [Engineering 2014], version 3.2.1, and were played back to the TV using the DekTec StreamXpress software utility.

Using our test setup, we were able to create HbbTV applications which ran invisibly in the background, as well as applications which completely took over the TV screen. Using HbbTV, we were able to deploy the Browser Exploitation Framework (BeEF) Toolkit [development team 2014] on the TV and use it to port scan the TV's intranet, examine the TV's runtime environment and display fraudulent login messages on the TV. We were able to crash the TV by having it render a malformed image file – a precursor for exploit distribution. Finally, we were able to craft a denial of service attack on an external web server, which ran as long as the user was tuned in to a particular channel. We verified that we were able to access servers both on the Internet at large and on the local intranet.

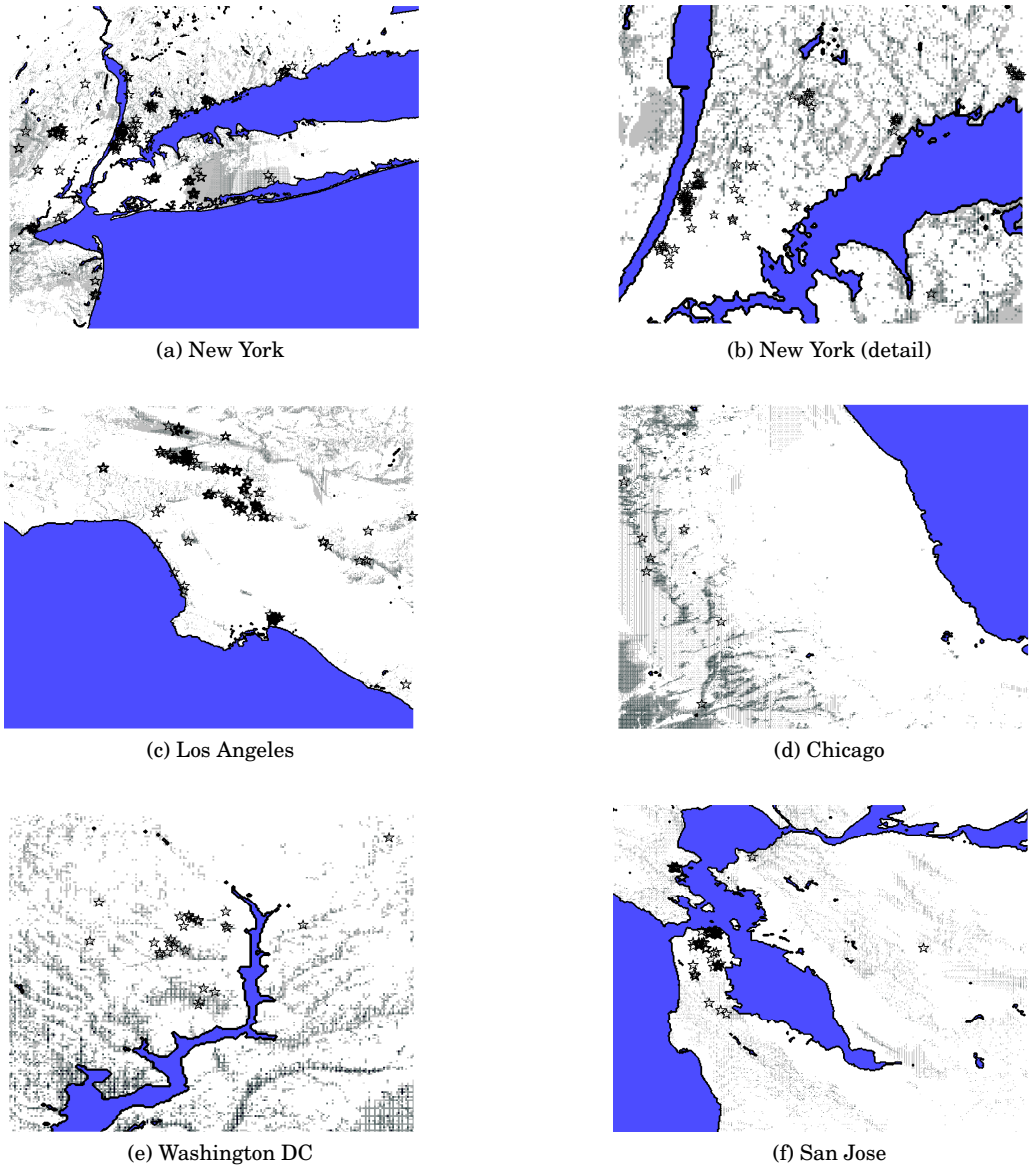
8. DISCUSSION

8.1. Risk Assessment Analysis

Table IV summarizes the attacks described in this paper and assigns each one with a qualitative complexity and damage potential. The justification for each qualitative complexity and damage assessment grade is provided below. In our analysis we assume the attack setup costs $450 in fixed costs, and that each attack costs an additional $50 per hour in variable costs (including equipment running costs and compensation for the risk taken by the attacker, who has to be physically close to the attacked location).

CMSA number	Largest City in CMSA	Population (2000 census)	NBC Station	CBS Station	ABC Station	Fox Station	CW Station
5602	New York, NY	21,199,865	WNBC (WVIT-DT) (WCAU) (WNYT)	WCBS-DT (KYW-TV)	WABC-TV (WTNH-DT) (WPVI-DT)	WNYW-DT (WTIC-TV) (WXXA-TV)	WPIX
4472	Los Angeles, CA	16,373,645	KNBC-DT (KNSD-DT)	KCBS-DT (KFMB-TV)	KABC-TV (KGTV-DT)	KTTV (KSWB-DT*)	KTLA-DT
1602	Chicago, IL	9,157,540	WMAQ-DT (WTMJ-DT)	WBBM-DT (WBBM-TV1) (WDJT-DT)	WLS-TV (WISN-TV)	WFLD-DT (WITI)	WGN-DT
8872	Washington, DC	7,608,070	WRC-DT (WBAL-TV)	WUSA (WJZ-TV)	WJLA-TV (WMAR-TV)	WTTG (WBFF)	WDCW (WNUV-DT)
7362	San Jose, CA	7,039,362	KNTV-DT (KSBW) (KCRA-DT)	KPIX-TV (KOVR) (KION-DT)	KGO-TV (KGO-TV1) (KXTV)	KTVU (KCBA-DT) (KTXL-DT)	KBCW (KMAX-TV)

Table I: Surveyed combined metropolitan statistical areas (data for KSWB-DT was not available for analysis)



(a) New York

(b) New York (detail)

(c) Los Angeles

(d) Chicago

(e) Washington DC

(f) San Jose

Fig. 5: Metropolitan locations vulnerable to an attack on one of the Big 5 stations

We conservatively assume that the attack impacts 10,000 hosts – as we showed in Subsection 3.1, the attack can be easily scaled by one or more orders of magnitude by using a higher-powered amplifier.

The **denial of service** attack is the attack with the lowest complexity, since it requires no research on the side of the attacker, neither of the TV nor of the site under attack. However, its damage potential is also low, especially since it is not cost effective. As anecdotally shown in [Büscher and Holz 2012], a DDoS attack involving more than 20,000 hosts costs approximately $5 per hour. However, it must be noted that since the

Metropolitan Area	Affected Land Area (km^2)	Affected Land Area %	Affected Population	Affected Population %
New York, NY	3,127.2	11.6%	2,839,000	13.4%
Los Angeles, CA	1,657.6	1.8%	1,387,000	8.4%
Chicago, IL	3,720.1	20.7%	1,014,000	11.1%
Washington, DC	4,208.5	17%	1,772,000	23.3%
San Jose, CA	626.2	3.2%	358,000	5.1%

Table II: City-scale results of "big five" survey

TV-based DDoS attack described here is localized to a single area, it can overwhelm a single edge node on a Content Distribution Network and thus deny service to other users in the same physical area.

The **unauthenticated request forgery** attack (in which an attacker uses HbbTV to vote in a poll, promote an article, or click an advertisement) also has low complexity, since it only requires minimal reverse engineering of the target web page. However, it has a higher damage potential than the DDoS attack, since it is much easier to monetise due to the possibility of click fraud [Hansen 2007]. According to Google's official figures, the average cost per click to advertisers in 2013 was $0.94, out of which 25% goes to the fraudulent advertiser [Google Inc. 2013]. This means the attacker can expect an income of around $2500 per attack even if every compromised host clicks only a single ad. In addition, since the interactive abilities abused by this attack are the main selling points of HbbTV, this attack has a wider area chilling effect of scaring advertisers and limiting the adoption of HbbTV.

The **authenticated request forgery** attack has a higher complexity than the previous two attacks, since it requires the attacker to discover and exploit a situation in which credentials are shared between the HbbTV runtime and other applications running on the Smart TV. However, this attack has a higher damage potential, since webmail and social network accounts are easier to monetise. According to [Thomas et al. 2013], a username/password pair for a verified Facebook account can be sold on the black market for as much as $1.50. The attack as described does not capture these credentials, but rather a local, short term session identifier. While the market value of this session identifier is no doubt less than the full credentials, it will still allow an attacker to act on the victim's behalf for a short period. This stolen credential is easy to exploit in our specific threat situation, since the malicious content originates from the victim's own IP address, which was typically associated by the service provider with this user. Interestingly, the HTTPOnly flag, which prevents Javascript code from accessing cookies, and protects against some forms of credential theft, is not effective against this attack. This is because the victim's web browser, which does have access to HTTPOnly cookies, is carrying out the attack on the attacker's behalf. The value of the credentials stored on the television, and therefore the impact of this attack, is expected to in the near future as users begin using their Smart TVs for additional activities such as shopping or health monitoring.

The **intranet request forgery** attack has medium complexity, since it involves compromising and exploiting not only the TV but also an intranet-connected device such as a router or a printer. However, there are existing intranet attacks which can

Location	Approx. Coordinates	Pop. Density (Persons/ km^2)	Stations Under Attack	Signal Strengths (dB)
Inwood, Manhattan, New York, NY	40.866, -73.924	80,300	Telemundo, Univision, CBS, NBC, Fox	-51.8, -52.1, -52.3, -55.3, -56.8
Ossining, NY	41.155, -73.868	41,800	PBS, CW, CBS, Telemundo, Univision	-56.6, -56.7, -57.9, -58.1, -61.0
NoMa, San Francisco, CA	37.795, -122.407	41,200	NBC, CBS, PBS, Fox	-52.6, -53.2, -55.6, -58.5
Pomona, LA County, CA	34.049, -117.816	39,300	Fox, ABC	-52.4, -52.5
Chinatown, San Francisco, CA	37.797, -122.411	36,600	CBS, NBC, PBS, Fox	-52.4, -55.2, -55.4, -57.9
West Chicago, IL	41.905, -88.207	24,000	Fox, ABC, Univision, CW, Telemundo, NBC, CBS, PBS	-50.7, -51.1, -51.3, -52, -54.0, -55.8, -58.6, -59.1
Long Beach, LA County, CA	33.778, -118.170	24,400	ABC, CW, Fox, NBC	-50.8, -57.0, -58.0, -60.6

Table III: A sampling of remarkably vulnerable locations

Attack Type	Complexity	Damage Potential	Overall Risk
Denial of Service	Low	Low	Medium
Unauthenticated Request Forgery	Low	Medium	High
Authenticated Request Forgery	Medium	High	High
Intranet Request Forgery	Medium	High	High
Phishing/Social Engineering	High	High	Medium
Exploit Distribution	Medium	High	High

Table IV: Risk assessment matrix of suggested attacks

be reused for this purpose. The damage potential of this attack is understandably high, since it lets the attacker compromise the user's personal computer.

The **phishing/social engineering** attack may be technically easy to launch, but it has external factors which make it more complex to carry out. First, the user's cooperation is required for this attack to succeed, raising the chance that the attack is ignored or, in the worst case, reported to law enforcement. In addition, the attack requires the attacker to set up additional attack infrastructure (e.g. a web server for collecting credentials), raising the risk of capture. The damage potential of this attack, however, is the highest of all attacks described here, since it risks the user's personal safety.

The **exploit distribution attack** may appear to be technically the most complex attack described here. However, since Smart TVs are commonly built using open-source components, an aspiring attacker can use an exploit patched in the most recent version of the component and not yet updated in the Smart TV. This attack has a high damage potential, since it results in total compromise of the TV.

8.2. Attacking cable and satellite

The attacks described in this paper all focus on content delivered over digital terrestrial television (DTT). According to [European Commision 2013], this is the most common delivery method for digital television across Europe. The DTT delivery method is the most amenable to our attacks, since the transmission channel is not authenticated and thus can be easily and cheaply subverted by the attacker. However, it must be noted that there are several areas of the world, most notably the USA, where this form of delivery is less common than cable or satellite communications.

There are several approaches which can be used to inject malicious content into cable or satellite digital TV. First, the attacker may try to attack the physical layer, either by sending a signal to the device antenna (in the case of satellite) or splicing into the microwave RF distribution network (in the case of cable). In contrast to DTT, the physical-layer transport of these systems may be scrambled or encrypted, giving additional difficulties to the attacker.

In another avenue of attack, the attacker can attempt to somehow compromise the content-delivery servers which insert benign HbbTV content to cable and satellite subscribers, then replace the benign application with malicious applications of his choice. Herfurt in [Herfurt 2013b] analyzed the content-delivery servers used by several German broadcasters and concluded that they might be vulnerable to traditional web-based attacks.

The last and most audacious approach would be for an attacker to buy a local TV station altogether. This will let the attacker overtly control all HbbTV content delivered by the station to potentially hundreds of thousands of viewers. As extravagant as this attack sounds, there has been a published case in which an organized crime family purchased a local telephone company for the purpose of performing fraud [Margolies and Reeves 2006]. Needless to say, a state-level player is also in a good position to in-

stigate this attack, commandeering all televisions in the country for inward or outward facing activities. For example, all televisions in a certain country might be ordered to participate in a state-sponsored DDoS attack or to promote a government-authored propaganda piece on social media.

8.3. Countermeasures

As stated in Section 3.2, there are three main security weaknesses in HbbTV: the limited user control over the application's life cycle; the flawed implementation of the web origin concept; and the differences in expectations deriving from the combination of the Internet medium and the broadcast RF medium.

This subsection proposes several approaches which can be used to address these weaknesses. Some of these defenses "break the standard" and make existing use cases for HbbTV applications (such as tracking cookies) impractical. Other defenses are less disruptive and can be independently deployed by security-minded equipment vendors and even marketed as differentiating features of their TV sets. The system-level solutions we propose for these flaws are applicable to designers of many classes of cyber-physical systems.

8.3.1. Crowdsource detection of RF attacks . Acting alone, an individual television set can do little to detect that its broadcast TV signal is suddenly coming from a malicious source. However, multiple television sets in the same area can aggregate their statuses, making it possible to use this information for detecting radio-based attacks. For example, if the Receive Signal Strength Indication (RSSI) in a certain geographic area has rapidly and suddenly changed, it might mean these TV sets are now receiving a signal from the attacker and not from the original radio tower. The RSSI information can even be used as a form of triangulation, to help pinpoint the exact location of the attacker and aid in his capture. Similarly, if multiple television sets are tuned to the same broadcast frequency, but a certain subset is receiving a different HbbTV application associated with this channel than the other TVs, this can indicate that an attack is in progress. It would be interesting to find a way of achieving this without compromising the privacy of the viewers.

8.3.2. Tighten control over app life cycle. The attacks described here are especially effective since they turn on automatically and without the knowledge of the user, and have no standard way of being disabled. The obvious way of addressing this limitation would be to guarantee the user's informed consent before active HTML content is rendered by the television. A good analogue to this behavior be found in the WHATWG's recommended implementation of the HTML5 full-screen API [van Kesteren and Çelik 2014], which specifies that "User agents should ensure, e.g. by means of an overlay, that the end user is aware something is displayed fullscreen. User agents should provide a means of exiting fullscreen that always works and advertise this to the user." In this spirit, the TV should prompt the user to press the red button **before** rendering any form of HbbTV content for the first time for a given channel, then periodically remind the user that content is running (for example by displaying a brief notification overlay whenever the user switches back to the channel). Users should also have a way of stopping HbbTV rendering for a particular channel.

This countermeasure is perhaps the most intuitive and can be immediately implemented by individual hardware makers. Sadly, it was shown that users do not react productively to warning messages which interfere with their browsing (or TV watching) [Sunshine et al. 2009]. In addition, there are already several established market players who will resist any change to this behavior, as they already use invisible HbbTV applications for user tracking and analytics.

8.3.3. Prevent broadcast-delivered HTML content from accessing the Internet. It is risky to allow unauthenticated broadcast content to define its own web origin. It seems tempting, then, to create a special restricted origin for broadcasted content, which is distinct from all other Internet domains. Another possible countermeasure is **content signing**. With this proposed defense, all HTML content delivered inside the DVB stream will be accompanied by a signed certificate attesting to its web origin. A malicious adversary cannot sign web pages on behalf of the website under attack, and thus cannot claim these sites as its origin. Unfortunately, even if all broadcast content was properly assigned to a restricted web origin, many attacks would still be possible via "blind" CSRF or PuppetNet attacks [Lam et al. 2006]. These attacks can cause considerable damage, even if the same-origin principle is upheld, by the sheer virtue of being able to access the Internet using somebody else's computer.

The HbbTV specification conceived the embedding of web content into the DVB data stream as a redundancy method, designed to allow the delivery of interactive content to the 30% of smart TV owners who do not, in fact, plug them into the Internet. This reasoning can be turned into an brutal, but effective, way to secure HbbTV. We recommend to **completely cut off Internet access** to all broadcast-delivered HTML content. Under this model, broadcast-delivered applications will be able to interact only with broadcast-delivered resources, while the only way of getting the television to access the Internet would be through an application delivered in URL form and fetched from the Internet itself. We note that the Google Chrome browser applies a very similar security policy to its browser extensions [Google, Inc. 2014].

8.3.4. Ineffective countermeasures. There are several defensive steps which appear at first to protect against the attack, but whose practical effectiveness is very limited. The first is **content encryption**. Rights-managed DVB content is commonly encrypted, or scrambled, and this encryption appears to be a way of preventing an attack which modifies the television channel. DVB encryption is, however, only applied to individual transport streams such as audio or video. The DVB specification [European Broadcasting Union 2011] dictates that and not to the program management table (PMT), which points to the HbbTV application, is always sent in the clear. This makes it possible for an adversary to inject a malicious application into any channel, even one with encrypted video and audio.

It will also be ineffective to protect against this attack using **Internet proxies**. As suggested by Tews in [Ghiglieri and Tews 2014], these "green button" proxies can deliver "sanitized" versions of HbbTV applications to users, after applying modifications which protect the security and privacy of the users. Unfortunately, these proxies are only effective as long as the HbbTV application itself lives on the Internet. Our attack deals with a different form of delivery, where the application resides inside the broadcast television stream.

8.4. Designing a Secure Internet-connected Sensor

It is interesting to note, that none of these flaws we discuss are directly specific to the television-based system we surveyed. Similar issues can also be found in other cyber-physical systems such as health sensors or augmented reality devices. It is therefore interesting to generalize the lessons we learned to other classes of cyber-physical systems where sensors are connected to the Internet.

To address the issue of life cycle management, users should always have a clear understanding of when and why a device is accessing the network or executing code, and how this execution can be paused or terminated. This is especially important for devices which users have a perception of understanding, based on their past experience with older non-connected devices. In our particular experience, the existence of the red

button the remote control led users to believe that an application does not actually execute until this button is pressed. A similar situation may exist in sensor systems whose user interface elements can be turned on and off by the user, but whose sensing mechanism is always on. For example, users might mistakenly think that turning off a device's screen will also turn off its radio.

To better follow the web origin concept, devices which render HTML content from non-Internet origins should severely restrict the access rights of this content, both between the content and the Internet and between different RF-sourced content items. If feasible, it is recommended that devices include two isolated web runtime environments, dedicating one to rendering only RF-sourced content.

To better separate the RF/sensory medium from the Internet medium, devices should also be designed to identify which network activities are the result of sensor or RF activities, and which are the result of explicit user action. The devices should then isolate and restrict data and control flow between the two domains. For instance, if a user explicitly visits a web site on his device and as a result is handed a cookie by the remote web server, this cookie should not be sent back to the web site if it is implicitly visited as the result of an RF-sourced activity.

A higher-level problem, which may also be prevalent in other cyber-physical systems, is that it is difficult to incentivize the defenses. In many of the attacks described in this paper the device owners are neither harmed nor even aware that an attack is in progress. The victims, in fact, are not the device owners, but rather third-party agencies such as websites or advertisers. This gives equipment vendors little cause to build countermeasures into their devices. This can be contrasted with DRM schemes whose circumvention directly hurts the equipment vendors's bottom lines. Successfully protecting against this class of threats thus requires system-level incentives and deterrents that will make it worthwhile for vendors to invest in creating defenses. One possible incentive would be for websites to identify and block all HbbTV accesses unless the protocol is fixed. Similarly, advertisers may reduce their payments to HbbTV-accessible websites publishing ads due to the increased risk of fraud. Finally, just like carmakers are culpable to accidents caused by unsafe cars, lawmakers can make it possible to sue TV manufacturers for losses which may are the result of insecure HbbTV implementations.

8.5. Related Work

Works investigating other security issues with Smart TVs were published by Grattafiori and Yavor in [Grattafiori and Yavor 2013] and by Lee and Kim in [Lee 2013]. The first academic work to deal with security weaknesses in HbbTV was published by Tews et al. in [Ghiglieri and Tews 2014; Ghiglieri et al. 2013]. This work focused on potential privacy leaks resulting from the use of HbbTV. The authors showed how an adversary sniffing encrypted traffic generated by HbbTV on a user's wireless network can infer which program the user is currently watching, even without decrypting the packets. This work also suggests a proxy-based method for blocking autostart applications from running on the television without user permissions.

Another series of works on HbbTV was published by Martin Herfurt [Herfurt 2013b; Herfurt 2013a]. Herfurt surveyed the HTML applications used by German HbbTV providers, discovering that many of them use HbbTV to periodically "phone home" and notify that the user is tuned to the station. Since this was done without the user's consent, these behaviors were considered a breach of German privacy laws. Herfurt additionally suggested a series of attacks which might be possible using HbbTV, including content spoofing, intranet attacks and even bitcoin mining. Finally, Herfurt also implemented a DNS-based privacy protection method called HbbTV Access Limiter (HAL).

Our work significantly contributes to that of of Herfurt and Tews et al. in two aspects. First, our work is the first to present and evaluate a cost-effective method of injecting malicious content into HbbTV systems, by using an RF-based man-in-the-middle attack. Second, our work is the first to call attention to the flawed specification of the same-origin policy for embedded HTML content, and to the devastating cross-domain attacks made possible by this flaw. It is the combination of a feasible attack model and a faulty security model which makes the attacks described in this paper so practical and so dangerous.

The most troubling attacks we discuss result from a flawed implementation of the Same-Origin Policy. As described by Johns et al. in [Johns et al. 2013], there have been several historical compromises of this policy, starting from 1996 [Felten et al. 1996], with each compromise resulting in serious consequences for web security. This work can be viewed as a particular instance of this case, made even more powerful due to the broadcast nature of the attack. Our work can also be viewed as a form of **cross-mechanism vulnerability**, in which the combination of perfectly benign broadcast and broadband systems create a system-of-systems with an **emergent property** which allows it to be compromised. Similar properties have previously been demonstrated in voice over IP systems which which combine Internet and PSTN networks [Keromytis 2012].

There have been several previous works which exploit a broadcast radio frequency channel to attack a multitude of computers. Notable are the work of Nighswander et al. which attacks GPS software stacks [Nighswander et al. 2012], and the work of Checkoway et al. which attacks car computers via the broadcast FM RDS channel [Checkoway et al. 2011].

9. CONCLUSION

We have described a series of novel attacks on Smart TVs – a widely deployed device whose significance in our life is only likely to grow. The key enabling factor of this attack was the fact that the device can render Internet content whose source is outside the Internet. This makes it possible for a physical attacker to cause a large-scale compromise of the Internet. We qualitatively and quantitively demonstrated that the attacks we described can be cost-effectively distributed to many thousands of users, and that they have a large damage potential. The attacks described in this paper are of high significance, not only because of the very large amount of devices which are vulnerable to them, but because they exemplify the complexity of securing systems-of-systems which combine both Internet and non-Internet interfaces. Similar cyber-physical systems will become increasingly more prevalent in the future Internet of Things, making it especially important to analyze the weaknesses in this system, as well as the limitations of its proposed countermeasures.

Acknowledgements: We thank our shepherd Srđan Čapkun, as well as the anonymous reviewers, for their helpful and instructive comments on the conference version of this paper. We also thank the reviewers of the journal version for their insightful comments. Erez Waisbard provided valuable information about MPEG internals. This material is based upon work supported by (while author Keromytis was serving at) the National Science Foundation. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

Advanced Television Systems Committee. 2008. ATSC Recommended Practice: Transmission Measurement and Compliance for Digital Television. Online. (May 2008). http://www.atsc.org/cms/standards/a_64b.pdf.

A. Barth. 2011. The Web Origin Concept. RFC 6454 (Proposed Standard). (Dec. 2011).

Adam Barth, Collin Jackson, and John C. Mitchell. 2008. Robust Defenses for Cross-site Request Forgery. In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08)*. ACM, New York, NY, USA, 75–88. DOI:http://dx.doi.org/10.1145/1455770.1455782

Armin Büscher and Thorsten Holz. 2012. Tracking DDoS Attacks: Insights into the Business of Disrupting the Web. In *Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats (LEET'12)*. Berkeley, CA, USA, 8–8.

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the 20th USENIX Conference on Security (SEC'11)*. Berkeley, CA, USA, 6–6.

Federal Communications Commission. 2001. Review of the Commission's Rules and Policies Affecting the Conversion to Digital Television. (January 2001). http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-01-24A1.pdf.

Advanced Television Systems Committee. 2014. A/105: ATSC Candidate Standard – Interactive Services Standard. (April 2014).

BeEF development team. 2014. The Browser Exploitation Framework. (January 2014). http://beefproject.com.

Avalpa Digital Engineering. 2014. OpenCaster: the free digital tv software. (February 2014). http://www.avalpa.com/the-key-values/15-free-software/33-opencaster.

European Broadcasting Union. 2011. Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems. ETSI TS 100 289 V1.1.1. (Sept. 2011).

European Broadcasting Union. 2012. Hybrid Broadcast Broadband TV. ETSI TS 102 796 V1.2.1. (Sept. 2012).

European Commision. 2013. Special Eurobarometer 396 – e-Communications Household Survey. (2013). http://ec.europa.eu/digital-agenda/en/news/special-eurobarometer-396-e-communications-household-survey.

Edward Felten, Andrew Appel, and David Walker. 1996. DNS-Based Attack on Java. (February 1996). http://sip.cs.princeton.edu/news/dns-spoof.html.

Open IPTV Forum. 2012. OIPF Specification Volume 5 – Declarative Application Environment. (September 2012). http://www.oipf.tv/specifications.

Marco Ghiglieri, Florian Oswald, and Erik Tews. 2013. HbbTV - I Know What You Are Watching. In *13. Deutschen IT-Sicherheitskongresses*. BSI, SecuMedia Verlags-GmbH.

Marco Ghiglieri and Erik Tews. 2014. A Privacy Protection System for HbbTV in Smart TVs. In *Consumer Communications and Networking Conference (CCNC), 2014 IEEE*.

Google Inc. 2013. Google Inc. Announces Third Quarter 2013 Results. (October 2013). http://investor.google.com/pdf/2013Q3_google_earnings_release.pdf.

Google, Inc. 2014. Chrome Extensions – Content Security Policy. (September 2014). http://developer.chrome.com/extensions/contentSecurityPolicy.html.

Aaron Grattafiori and Josh Yavor. 2013. The Outer Limits: Hacking the Samsung Smart TV. (July 2013). https://www.blackhat.com/us-13/briefings.html#Grattafiori.

Robert "RSnake" Hansen. 2007. Stealing Mouse Clicks for Banner Fraud. (January 2007). http://ha.ckers.org/blog/20070116/stealing-mouse-clicks-for-banner-fraud/.

Martin Herfurt. 2013a. Security Concerns with HbbTV. BerlinSides 0x04 Lightning Talks. (May 2013). http://mherfurt.wordpress.com/2013/06/01/security-concerns-with-hbbtv/.

Martin Herfurt. 2013b. Security Issues with Hybrid Broadcast Broadband TV. 30'th Chaos Computer Convention. (December 2013). https://events.ccc.de/congress/2013/Fahrplan/events/5398.html.

International Standards Institute. 2013. Information technology – Generic coding of moving pictures and associated audio information – Part 1: Systems. ISO/IEC 13818-1. (May 2013).

International Telecommunication Union. 2014. Planning criteria, including protection ratios, for digital terrestrial television services in the VHF/UHF bands. ITU R-REC-BT.1368. (Feb. 2014).

Martin Johns, Sebastian Lekies, and Ben Stock. 2013. Eradicating DNS Rebinding with the Extended Same-origin Policy. In *Proceedings of the 22nd USENIX Conference on Security (SEC'13)*. Berkeley, CA, USA, 621–636.

Martin Johns and Justus Winter. 2007. Protecting the Intranet Against JavaScript Malware and Related Attacks. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, Bernhard Hämmerli and Robin Sommer (Eds.). LNCS, Vol. 4579. Springer Berlin Heidelberg, 40–59. DOI:http://dx.doi.org/10.1007/978-3-540-73614-1_3

Hans-Joachim Kamp. 2013. 40 Jahre gfu. (June 2013). http://www.gfu.de/srv/easyedit/_ts_1373472398000/page:home/download/insightstrends/sl_1338454764893/args.link01/de_kamp.pdf.

A.D. Keromytis. 2012. A Comprehensive Survey of Voice over IP Security Research. *Communications Surveys Tutorials, IEEE* 14, 2 (March 2012), 514–537. DOI:http://dx.doi.org/10.1109/SURV.2011.031611.00112

V. T. Lam, S. Antonatos, P. Akritidis, and K. G. Anagnostakis. 2006. Puppetnets: Misusing Web Browsers As a Distributed Attack Infrastructure. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*. ACM, New York, NY, USA, 221–234. DOI:http://dx.doi.org/10.1145/1180405.1180434

American Radio Relay League. 2013. *2014 ARRL Handbook for Radio Communications* (91st ed.). American Radio Relay League. http://amazon.com/o/ASIN/1625950004/

SeungJin 'Beist' Lee. 2013. Hacking, surveilling and deceiving victims on smart TV. (July 2013). https://www.blackhat.com/us-13/briefings.html#Lee.

Dan Margolies and Greg Reeves. 2006. New York Man Sentenced for CassTel Mail, Wire Fraud Conspiracy. Online, *The Kansas City Star* January (2006). http://blogs.kansascity.com/crime_scene/2006/01/4_years_in_cass.html.

Mini-Circuits. 2010. ZHL-2010+ Low Noise Amplifier. Online. (December 2010). http://www.minicircuits.com/pdfs/ZHL-2010+.pdf.

National Vulnerability Database. 2011. CVE-2011-2107: Cross-site scripting (XSS) vulnerability in Adobe Flash Player. Online. (August 2011). http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2107.

Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley. 2012. GPS Software Attacks. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*. ACM, New York, NY, USA, 450–461. DOI:http://dx.doi.org/10.1145/2382196.2382245

Yossef Oren and Angelos D. Keromytis. 2014. From the Aether to the Ethernet - Attacking the Internet using Broadcast Digital Television. In *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014.*, Kevin Fu and Jaeyeon Jung (Eds.). USENIX Association, 353–368. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/oren

VideoLAN Organization. 2014. VLC media player. (February 2014). http://www.videolan.org/vlc/index.html.

QGIS Project. 2014. QGIS – A Free and Open Source Geographic Information System. Online. (June 2014). http://qgis.org.

Theodore Reed, Joseph Geis, and Sven Dietrich. 2011. SkyNET: A 3G-enabled Mobile Attack Drone and Stealth Botmaster. In *Proceedings of the 5th USENIX Conference on Offensive Technologies (WOOT'11)*. Berkeley, CA, USA, 4–4.

L. Seirup and G. Yetman. 2006. U.S. Census Grids (Summary File 3), 2000: Metropolitan Statistical Areas. (2006). http://sedac.ciesin.columbia.edu/data/set/usgrid-summary-file3-2000-msa

Ofer Shezaf. 2007. The Universal XSS PDF Vulnerability. Online. (January 2007). https://owasp.com/images/4/4b/OWASP_IL_The_Universal_XSS_PDF_Vulnerability.pdf.

Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *Proceedings of the 18th USENIX Conference on Security (SEC'09)*. Berkeley, CA, USA, 399–416.

The Diffusion Group. 2013. Connected TVs Now Present in Six of Ten US Broadband Households. (May 2013). http://tdgresearch.com/connected-tvs-now-present-in-six-of-ten-us-broadband-households.

The Nielsen Company. 2014. Local Television Market Universe Estimates. Online. (January 2014). http://www.tvb.org/media/file/TVB_Market_Profiles_Nielsen_TVHH_DMA_Ranks_2013-2014.pdf.

Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson. 2013. Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In *Proceedings of the 22nd USENIX Conference on Security (SEC'13)*. Berkeley, CA, USA, 195–210.

Anne van Kesteren and Tantek Çelik. 2014. Fullscreen API Living Standard. (September 2014). http://fullscreen.spec.whatwg.org.