A Privacy Protection System for HbbTV in Smart TVs

Marco Ghiglieri
Technische Universität Darmstadt
Darmstadt/Germany
marco.ghiglieri@cased.de

Erik Tews
Technische Universität Darmstadt
Darmstadt/Germany
erik.tews@cased.de

***Abstract*—The popularity of smart entertainment devices is growing every day. Products like blu-ray players, set-top boxes and Smart TVs (STV) with high connectivity are on the market. Many of them connect to the Internet via LAN or WiFi. Especially Smart TVs enable the broadcasting stations to provide real-time information directly to the consumers, for example additional information about a current TV program. HbbTV is one of the standards on STV for combining the two data media DVB and Internet. It defines how commonly used web technologies can be used as a transparent overlay over the current channel. Each respective broadcasting station is responsible for the contents of their channels' HbbTV signals.**

In this article, we describe how broadcasting stations measure the consumers viewing behavior more accurately using HbbTV. We show which technologies are used and which cause privacy risks, i.e., which methods lead to the exposure of personal preferences. Additionally, we describe a method how an evil-minded neighbor is able to monitor the viewing behavior without the user's knowledge and consent. This method is possible on most channels using HbbTV. It is not even required that the user actively starts the HbbTV application. Beyond that, we can collect this data on an encrypted WiFi network as well. Finally, we discuss our implementation for significantly reducing the privacy risk HbbTV poses.

I. Introduction

The popularity of smart entertainment devices is increasing every day and more and more devices are being connected to the Internet. Smart TVs (STV) or connected TVs are used to receive content comfortably from the Internet. STVs are connected to the Internet via LAN or WiFi. In Germany, it is assumed that by 2016 the total amount of households having at least one STV will have reached 20.1 million [1]. STVs connect two media: DVB (Digital Video Broadcast) and Internet. This introduces new and innovative technologies and functionalities on STVs.

HbbTV (Hybrid Broadcast Broadband TV) is one of the standards on STV for combining these two media. It enables the broadcasting stations to deliver additional interactive (broadcast dependent and independent) content directly to end users. The newest specification version 1.2.1 was released in November 2012 and approved by the ETSI [2]. It specifies the technical aspects of HbbTV and gives a detailed overview of how to develop an HbbTV application. In Germany about 13.4 million households (35% of all German households) are expected to have at least one device supporting HbbTV by 2016 [3]. The content delivered by HbbTV can be highly interactive, which provides some advantages for both users and advertisers. For example, a user can get videos from media libraries, weather information or additional information about a current program. A GfK survey stated that the acceptance of this medium is growing [4]. An advertisement provider, on the other hand, can deliver different advertisements for different regions. This allows advertisements to be more personalized and the coverage of an advertisement can be measured directly, e.g., a higher revenue of up to 930.000 Euro can be earned by Bavarian local broadcasting stations [3]. Each respective broadcasting station is responsible for the contents of their channels' HbbTV application.

Additionally, ARTE, a German/French TV station, expects HbbTV to replace the current teletext technology [5].

A. Outline and Our Contribution

This article is one of the first academic publications about HbbTV, especially about the privacy aspects of HbbTV (see Section II). We briefly introduce HbbTV (see Section III) and follow with an in-depth analysis (see Section IV) in regards to security and privacy. We show that many broadcasting stations and even neighbors are able to track users more accurately than before. We show in detail that

- in Germany and Austria tracking methods are used that enable neighbors and broadcasting stations to track users,
- many HbbTV applications transmit more information than they really need to work properly,
- it is possible for neighbors to track users even on an encrypted WiFi network

Recommendations will be shown in Section V and our own protection system is discussed in Section VI. All results are from a rather technical point of view and legal aspects are not covered in this publication.

II. Related Work

To the best of our knowledge, we are not aware of any other work related to security and privacy in HbbTV beside our German article presented on the German BSI national security conference [6]. However, some work is related to HbbTV in general. Lukac et al [7] discusses a technical implementation of HbbTV. Another paper described how to record and deliver HbbTV applications, so that the user may watch a program repeatedly with all the information available

978-1-4799-2355-7/14/$31.00 ©2014IEEE

[8] at replay time. Recently, many security issues have been found in STV subsystems. Auriemma reported a vulnerability where an STV is not usable when it receives invalid data packets at a specific network port [9]. More hacks for the underlying hardware or software were published by SeungJin researchers [10] and Mulliner and Michéle [11]. A manual was published outlining how to evaluate the security of your home entertainment system [12].

III. HbbTV Standard

ETSI approved the HbbTV standard in November 2012 [2]. The standard specifies the technical framework for HbbTV applications and how it should be implemented in Smart TVs. Basically, an HbbTV application is a website, which can be displayed as a transparent overlay over the current program. Thus, an HbbTV supporting STV implements an invisible (for the user) web browser that opens the HbbTV application from the Internet. The HbbTV application starts when the STV receives an URL in the DVB stream sent by the broadcasting station. The URL is then extracted from the DVB stream and will be loaded in background directly from the Internet. The content of this URL can be any web site on the Internet written with standard web techniques like HTML, CSS and JavaScript. The broadcasting stations typically provide a kind of landing-page URL of their HbbTV application, which displays the notification message that an HbbTV application is available and can be activated by pressing the *Red Button* on the remote.

In this work, we focus on broadcast dependent HbbTV applications, i.e., HbbTV applications that are started and loaded by switching to a channel with HbbTV signal in the DVB stream.

Figure 1 outlines the typical process of activating an HbbTV application. The user has different possibilities to start an HbbTV applications on the STV (see HbbTV standard for the full list). The most common way is that the HbbTV notification, which tells the user that an HbbTV application is available, is shown on the DVB program (2). If the user presses the *Red Button*, the HbbTV application starts in full screen mode (3).

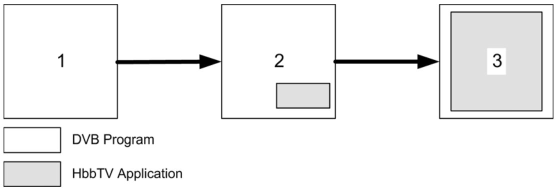

Fig. 1. Activation Process of HbbTV Application

Furthermore, it is specified that an HbbTV application should not start in full screen mode on a regular TV program. It should only notify the user that an HbbTV application is ready. No technical enforcement of this recommendation is in place, i.e. the broadcasting station can embed an auto-start application that starts in full screen mode when switching to a channel. Unfortunately, the current HbbTV specification does not provide information for security or privacy.

IV. HbbTV in the Real World

The HbbTV consortium is a pan-European initiative with the aim to harmonize the broadcast and broadband delivery of entertainment to the end consumer through STV and other set-top boxes [13]. We have already seen that HbbTV is used by many broadcasting stations in Germany and some in Austria (see table II in section IV-C). In 2012, we analyzed the HbbTV traffic of HbbTV over a period of six months. Channels without HbbTV were not analyzed since there is no extended privacy risk.

As a summary in this section, we show that HbbTV does not only represent an advantage for the user, but that it must be used carefully to avoid privacy issues. The current broadcasting method via DVB comes without a back channel to the provider or to third-parties, hence, it has no additional privacy issues. If an Internet connection is available and HbbTV is used, consumer behavior can be measured very accurately, because data is sent back via Internet.

A. Test Environment

The tests were performed on two Smart TVs from Samsung; UE40D6200 and UE40ES6300. Both devices can receive a signal via satellite, cable and terrestrial. The first STV was the reference model to double-check the findings on the UE40ES6300. Both STVs support HbbTV and call it *data service* in their menus.

In figure 2, the technical setup is outlined. The SmartTV (STV) is connected to both media, DVB and Internet. The Internet connection is established via WiFi. A PC, which is not part of the network, captures the raw packets using the tool Wireshark[1] (encrypted or plain) on the WiFi network. For the analysis in Section IV-C the encryption has been completely deactivated, so that the WiFi packets were directly readable by the PC. However, in Section IV-D the encryption of the WiFi network is set to WPA2; currently the standard to protect most home WiFi networks.

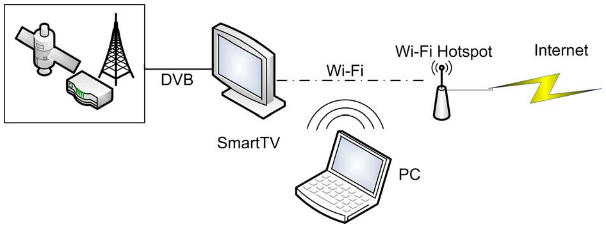

Fig. 2. Test Environment

In all scenarios, we gathered the data from the STV to the Internet and vice versa. This data was saved and then analyzed later on.

B. General Results

The traffic of all HbbTV channels was captured and compared with different broadcasting methods: cable, satellite and terrestrial. We found no significant differences between them,

[1] http://www.wireshark.org/

all results could be reproduced in all three broadcasting types. In the remainder we will therefore not differentiate between them.

For a better differentiation between exchanged packets, we divided them into the following time phases (see figure 3):

1. Phase:
   Time between switching to channel and the HbbTV notification is shown,
2. Phase:
   Time between displaying the HbbTV notification and when the *Red Button* is pressed by the user and
3. Phase:
   Executing the HbbTV application after pressing the *Red Button*. This phase has not been analyzed, since the user has actively started the HbbTV application by pressing the button and data exchange between the STV and the Internet is expected.

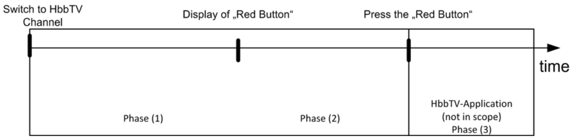

Fig. 3. Phases

Our paper mainly focuses on phases 1 and 2, in which the user has not intentionally activated the HbbTV application. We found on several channels with HbbTV two different request types (start-up and periodic requests) to the broadcasting stations, which we explain in the following paragraphs.

Start-up requests

When switching to an HbbTV channel (Phase 1), the broadcasting station provides an URL within the DVB stream to load the first HbbTV notification showing that an HbbTV application is available. We call this action *start-up request*. If no application is available, no URL in the DVB stream is provided and no further action is performed by the STV.

Periodic Requests

In addition to the start-up requests, we measured periodic requests after the HbbTV notification has been displayed (Phase 2). The time between each request differed from one second to 15 minutes depending on the channel. These requests are made before the user actively started the HbbTV application by pressing the Red Button (Phase 3), so the user does not expect any data to be transferred to some other party, e.g., broadcasting stations.

We detected channels with only start-up requests (see figure 4) and channels with a mixture of start-up and periodic requests (see figure 5). We explain our findings in Section IV-C.

However, the HbbTV application differs from channel to channel. For one broadcasting station it is only a replacement for teletext, for another it is a portal to deliver a variety of additional services such as media libraries or the possibility to watch previous content. The broadcasting stations are in all cases responsible for all requests and the content they provide to the users. We spotted no network activity, which would indicate that HbbTV applications access data from the STV vendors, for example to exchange data for statistical reasons or to identify STVs/users.

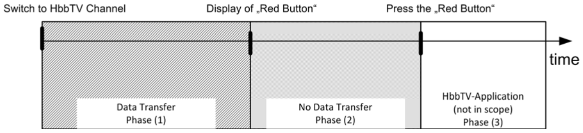

Fig. 4. Phases without Periodic Requests

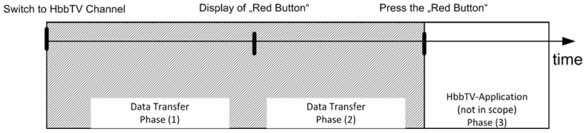

Fig. 5. Phases with Periodic Requests

C. Analysis On A Plain Text Network Channel

As mentioned above, this analysis has been performed on a WiFi network without any encryption, i.e., the data packets on the WiFi network could be captured directly and are human readable.

Start-up requests were measured after the STV has received an URL in the DVB stream, usually when switching to a channel with HbbTV signal. Our analysis has shown that periodic requests, if implemented in the HbbTV application, were made in a time period from one second up to 15 minutes. An in-depth analysis of the transferred packets in a periodic request has led to the following data categories: (a) Pre-loading of the HbbTV content or an application, (b) tracking methods or (c) (personalized) advertisements. We assigned the found characteristics of the captured packets to the groups A,B,C,D and Z (see table I).
Z is a group of channels, on which our STVs were not permitted to receive the HbbTV application. Some station offer their HbbTV service only for a restricted set of devices. Our Samsung STV was not allowed to use this service, but some initial start-up requests could be gathered on this channel group.

A is basically a group of channels where the start-up request is performed to show the HbbTV notification. Group B that has all characteristics of group A, loads the HbbTV application content before the user has pressed the *Red Button*. The content pre-loading is done with periodic requests. Third party tracking scripts such as Google Analytics are the additional characteristic of group C. Group D, as the most privacy invasive channel group in our test, has channels assigned which are displaying (personalized) advertisements to the users in certain time periods,e.g., 15 minutes.

We assigned the channels from Germany and Austria depending on their characteristics to the groups (see table II). Table II is not complete and only represents our results. Even

Characteristics/Group	**A**	**B**	**C**	**D**	**Z**
HbbTV	x	x	x	x	x
Single request	x	x	x	x	x
Periodic requests		x	x	x	?
Tracking					?
Data transferred to third parties			x	x	?
Personalized Ads				x	?
WPA2-Tracking	x	x	x	x	x

TABLE I
GROUPS OF CHANNELS

Group	**Channel**
A	ZDF (HD), ZDF Infokanal, ZDFneo, 3Sat (HD), Bibel TV, QVC (HD)
B	ARD-Gruppe (Erste (HD), hr-fernsehen, SWR, SR, rbb, EinsPlus, EinsExtra, EinsFestival, WDR, NDR, MDR, SWR, MDR, br alpha, Phoenix (HD), br
C	ProSiebenSat1-Gruppe(Pro Sieben, Kabel 1, Sat 1), ARTE (HD), Puls 4 Austria
D	Anixe (HD), Anixe iTV
Z	RTL, VOX

TABLE II
CHANNEL ASSIGNMENTS

if the table is limited to Germany and Austria, HbbTV is standardized for Europe and can be implemented by other broadcasting stations in the near future as well.

Next, we explain the traffic flow for each station group (see table II). The initial HbbTV request is transferred by the DVB stream and triggers the Smart TV to load a specific URL from the Internet. An HbbTV notification, including a text and a channel logo is provided in return. In the background a variety of scripts and images are transferred to perform the start-up-request. If the previous requests are performed successfully, the notification that the HbbTV application is ready and can be activated by the *Red Button*, is displayed to the user (valid for sender groups A-D in table I).

In the sender groups B-D, we have seen periodic requests before the user pressed the *Red Button*. These requests to the server of the broadcasting stations are in an interval from one second to 15 minutes. The interval length varies from channel to channel. Such requests in the Internet are used for pre-loading content or tracking users very accurately. A pre-loading method in a high frequency manner is technically not needed, since the server load increases dramatically and the possibility to track users is significantly higher. This allows the broadcasting station to check if a user still has a specific channel selected. In the channel group C and D we found several tracking scripts in the traffic, such as Google Analytics, Chartbeat.com and Webtrekk. The purpose of these services is clearly defined, they should track user behavior and collect data of the user's device. The user, however, does not expect any interaction with the Internet before he/she activates an additional service, e.g., an HbbTV application. In the time, where a Smart TV receives or sends (hidden) HbbTV content from/to the Internet, the channel must be turned on, since the specification requires that behavior. When the channel is switched, the HbbTV signal changes and the current action of the HbbTV browser will be interrupted.

We do not know how the gathered data is processed by the broadcasting stations, but even just the possibility to collect a variety of data is a high privacy risk for users. The data can be used to gather user behavior in real time with more accuracy than ever before. In group D, the most privacy invasive group of channels, we measured full screen advertisements every 15 minutes. We uncovered geo-location data in the data sent to the broadcasting station. This does not add an additional privacy risk, since the geo-location data can be determined by the IP address. However, a user does not expect this to happen.

Most Internet service providers assign an IP address for 24 hours to a user, which makes the user unique and identifiable within that period. Even afterwards users can be identified by using cookies with IDs, but our test devices have not saved any cookies or returned the cookies to the server. It is not further analyzed if this is a security feature or a bug in the implementation of the STV. If an STV would accept the cookie and send it back to the broadcasting station, it would be easily possible to track a user even if the IP address changes.

Summarizing, we found no data which can be directly used to identify users, e.g., user logins, credit card numbers or similar. But broadcasting stations which provide more than one channel may track the user viewing behavior over these channels, i.e., it is possible to determine a user's preferences or political orientation over these channels. Furthermore, data to identify an STV are transferred, for example screen resolution, vendor, IP address and cookies. For the future, it is likely that additional services for HbbTV will implement user logins for user identification and even access to web cams or motion sensors are possible.

D. Analysis On Encrypted Network Channel

In this Section we analyzed the fact that periodic requests happen in-depth and show that a neighbor is able to track the signal even on a WPA2 encrypted WiFi network. We call this user attacker. She/he can determine the usage of an HbbTV channel accurately. The attacker must be in the range of the WiFi signal and does not need the encryption key or be a member of the network.

In WPA2, AES-CCMP or TKIP is used to encrypt the network packets. In both methods (and WEP) the plain text is being encrypted with a stream cipher (RC4 with WEP and TKIP, AES with Counter-Mode in AES-CCMP). Additionally, a block with fixed length to protect the integrity is appended. A padding, as used for example with block ciphers masking the real length of a data packet, is not used. Even the MAC-Address of the sender resp. the recipient of the packet is transmitted unencrypted. An attacker can thus identify the vendors of all devices in a WiFi network, and the length of the plain text packets of the encrypted data packets [14].

All HbbTV applications we analyzed consist of a GUI, which does not change very frequently, and configuration files that depend on the current program and change very frequently. All data is transferred via HTTP. On the STV side, the start-up and periodic requests differ in the user agent. In return to these requests the server's content had mostly the same size.

The amount of received data and the size of each data packet differs from channel to channel. In order to detect the HbbTV channel over the encrypted WiFi Channel we used the following technique: (1) An attacker uses his/her own Smart TV to create a list of all HbbTV channels with a typical size and length of packets. Packet sizes found on more than one sender, are ignored. Packets belonging to data that is usually cached by the browser will be filtered and removed. (2) The attacker now captures the whole encrypted data stream of the victim. With the help of the MAC address he can filter the data stream according to the device and find only the STV. Another filter removes all data packets, which have full MTU (maximum transmission unit) length. With a sliding window method all packets are captured that were within a time interval of 10 seconds, i.e, packets of the previous 10 seconds are analyzed. If most captured data packet sizes are contained in the list created in (1), it is very likely that this is a specific channel running on the STV. In our experiments we had no false positives, however, sometimes instead of identifying the individual channel, the channel group was identified. This behavior was always tested live on the channels listed in table II and only the key packet sizes were extracted from saved data.

A channel being turned on for only a few seconds turned out to be a problem. The HbbTV data was only partially loaded and we were not able to recognize the channel.

If the Internet connection is done over DSL with PPPoe or VPN and the STV cannot use the full packet size of 1500 bytes, the list must be modified, so that the characteristics are aligned to the new MTU. A possible extension of the attack technique would be to add timing information to the analysis. However, we had not implemented this extension, since we had a high probability to recognize the right channel or channel group.

V. Recommendations

Smart entertainment devices with more and more connectivity options are flooding the market, but as of now are not common in every household. The techniques used in these devices have been used for many years already in devices such as computers or laptops. However, in smart entertainment devices it opens up new innovative functions for the users. Often security and privacy play a secondary role in the development of such devices. We introduce three fields of recommendations and group them by their place of modification: HbbTV specification, in the device or in the application.

A. HbbTV Specification

We have analyzed the current version of the HbbTV specification and found no paragraph, which states that privacy by design is an important development concept and should be considered while developing an HbbTV application. The specification should be extended so that there is a catalog of guidelines, which indicates on how to implement privacy, for example a list of functions or techniques would be desirable that may be used without privacy issues before pressing the *Red Button*. Moreover, in order to avoid channel identification after the start-up request, the HbbTV specification could standardize the data packets in size or characteristics before pressing the *Red Button*, even an encryption scheme with padding is possible. In other words, techniques for normalizing the size of the transferred data packets are needed, which in turn leads to indistinguishable data packets. Third party tracking scripts like Google Analytics should be forbidden before the user actively presses the *Red Button*.

B. Device Modification

As known from other devices, the browser is accessing webpages on the Internet and in the example of an STV the HbbTV content. We found that the functionality of these STV browsers are different from those of usual devices, because the functionality is lower; cookie management or the possibility to implement add-ons are not available, which would lower the privacy exposure. For example, in current desktop PC browsers add-ons for different purposes can be used, for example Adblock, Noscript. These add-ons are not available for STV since the STV browsers do not support it.

The option to activate and deactivate HbbTV is called *data services*, which is per default deactivated. When activating it, the possible risks are not being mentioned. A more fine-grained option to activate or deactivate HbbTV for each channel would let the user decide from what channel he/she likes to see the HbbTV content. This would minimize the risk to be tracked by a third party (see our implementation in Section VI). A more restrictive approach is to avoid receiving any data from the Internet before the *Red Button* is pressed. Instead of loading the notification that an HbbTV application is ready directly from the Internet, the STV could deliver a uniform *Red Button*, which will be shown whenever an HbbTV signal is detected in the DVB stream. However, the possibility to individualize the *Red Button* notification is lost and and the channels' logos are not shown to the user. Maybe caching mechanisms can help to maintain the possibility of individualization, while at the same time preserving the users' privacy.

C. HbbTV Application Modification

HbbTV applications should follow the privacy by design approach and minimize the data sent to the server. The user should have the option to decide if tracking scripts may be used or not. This consent could be made with a cookie on the STV. The HbbTV applications must then respect this flag. Another method, which is disabling the data services, would deactivate the complete advantage of HbbTV. In most cases it is worth to develop a method to be more privacy-friendly, since the variety of information and content is very high.

VI. Our Implementation - HbbTV Privacy Protector

In order to counter the problems mentioned above, we developed the HbbTV Privacy Protector (HPP). Our implementation consists of a transparent HTTP proxy server, that intercepts traffic between the Smart TV and the internet uplink. When a new HbbTV application is detected (for example when changing a channel and thereby autostarting a new HbbTV application), the request is intercepted and forwarded to our local webserver. Our local webserver delivers an HbbTV application, which waits until the user actively enables HbbTV by pressing the *Green Button* on his/her remote. We have not chosen the *Red Button* to not confuse users. When that happens, the interception rule is removed from the proxy server and the user is forwarded to the broadcaster's HbbTV application.

Our implementation is based on *mitmproxy*, a lightweight HTTP and HTTPS interception proxy written entirely in python. We used a custom python script to add the HbbTV interception functionality to *mitmproxy*. Traffic redirection can be done transparently on a Linux device between the Smart TV and the internet uplink using the Linux *iptables* tool. Right now, the list of HbbTV URLs is hardcoded in the implementation, but could also be autodetected by analyzing content types in HTTP requests and responses.

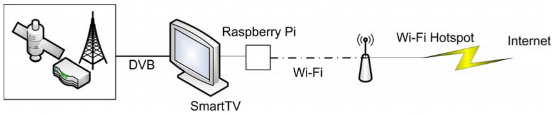

Fig. 6. Architecture of the HPP

We developed the tool compatible with the *Raspberry Pi* platform, a small ARM based computer that is quite popular for building TV media centers. Smart TV Internet traffic needs to be routed through the *Raspberry Pi* for example using the Internet connector, and can then be passed on to the local WiFi using a USB WiFi adaptor (see Figure 6). Due to the HDMI connector with HDMI-CEC support, the *Raspberry Pi* can be controlled and configured from the Smart TV using the TV remote. The small device size makes it possible to mount it on the TV backside, out of sight.

We are planing to make the *Raspberry Pi* version of the tool available for the public. This will include a manual and an explanation how easily it can be set up.

VII. Conclusion

In this paper we demonstrated that HbbTV can be used by broadcasting stations and neighbors to track users. We did not expect that the tracking of users would be so easily possible. According to our analysis the privacy risk is severe, since the tracking mechanisms cannot be deactivated easily. In standard STV models deactivating data services for the whole TV would be a feasible way, which, however, would turn a Smart TV into a regular TV without any additional functions. The privacy issues are not caused by implementation errors of the TV vendors, only the HbbTV application providers are responsible, i.e. the broadcasting stations.

The broadcasting stations have the possibility to get more accurate usage numbers, which can be measured almost in real time. Moreover, personalized ads can be delivered to the users.

We have communicated the results to different broadcasting stations. Only one broadcasting station has agreed to communicate with us to solve the problem.

Acknowledgments

We thank Florian Oswald for his support; he wrote his Bachelor Theses in the context of this project. We also thank Birgit Blume for her work to get this paper finished.

This work was supported by the *European Center for Security and Privacy by Design (EC SPRIDE),* funded by the German Federal Ministry of Education and Research (BMBF), and the *Center for Advanced Security Research Darmstadt (CASED),* funded by the LOEWE program of the Hessian Ministry for Science and the Arts (HMWK).

References

[1] Goldmedia , " Statista, Anzahl der Smart TV-Haushalte in Deutschland im Jahr 2010 und Prognose bis 2016 (in Millionen) ," Oct. 2011, http://de.statista.com/statistik/daten/studie/208236/umfrage/prognose-zur-entwicklung-der-smart-tv-haushalte-in-deutschland/.

[2] IRT GmbH, "HbbTV Specification (approved by ETSI as ETSI TS 102 796 v1.2.1 in November 2012)," http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.02.01_60/ts_102796v010201p.pdf.

[3] BLM, Goldmedia , " Statista, Anzahl der Haushalte (in Mio.) mit mind. einem an das Internet angeschlossenen TV-Gerät von 2011 bis 2016 ," Oct. 2011.

[4] GfK , " Statista, Welche der folgenden Funktionen nutzen Sie mindestens 1x täglich bzw. mehrmals pro Woche auf ihrem Smart-TV ? ," Nov. 2011, http://de.statista.com/statistik/daten/studie/223465/umfrage/nutzung-von-internetfaehigen-tv-geraeten/.

[5] ARTE G.E.I.E. , " HbbTV - Der Standard für hybrides Fernsehen ? ," Jun. 2011, http://www.arte.tv/de/2153564,CmC=3977990.html.

[6] Marco Ghiglieri, Florian Oswald, Erik Tews, "HbbTV - I Know What You Are Watching," in 13. Deutschen IT-Sicherheitskongresses, Secu-Media Verlags-GmbH, May 2013.

[7] Z. Lukac, M. Radonjic, B. Veris, T. Maruna, and N. Kuzmanovic, "The experience of implementing a hybrid broadcast broadband television on network enabled tv set," in *MIPRO, 2011 Proceedings of the 34th International Convention*, May, pp. 840–844.

[8] J.-C. Dufourd, S. Thomas, and C. Concolato, "Recording and delivery of hbbtv applications," in *Proceddings of the 9th international interactive conference on Interactive television*, ser. EuroITV '11. New York, NY, USA: ACM, 2011, pp. 51–54. [Online]. Available: \url{http://doi.acm.org/10.1145/2000119.2000129}

[9] L. Auriemma, "Endless restarts," Apr. 2012, http://aluigi.altervista.org/adv/samsux_1-adv.txt.

[10] L. SeungJin, "Dirty note on Samsung Smart TV Security," Dec. 2012, http://beistlab.files.wordpress.com/2012/12/samsung_smart_tv_attack_surfaces2.pdf.

[11] C. Mulliner and B. Michéle, "Read it twice! a mass-storage-based tocttou attack." in *WOOT*, 2012, pp. 105–112.

[12] Rikke Kuipers, Eeva Starck & Hannu Heikkinen, "Smart TV Hacking: Crash Testing Your Home Entertainment," http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-smart-tv-fuzzing.pdf.

[13] IRT GmbH , " HbbTV = More entertainment at your command ," http://hbbtv.org, accessed on 02.04.2013.

[14] IEEE, " Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)," pp.1-2793, March 29 2012 doi: 10.1109/IEEESTD.2012.6178212 .