Smart-TV security: risk analysis and experiments on Smart-TV communication channels

Yann Bachy, Vincent Nicomette, Mohamed Kaâniche, Eric Alata

Noname manuscript No.
(will be inserted by the editor)

Smart-TV security

Risk analysis and experiments on Smart-TV communication channels

Yann Bachy · Vincent Nicomette · Mohamed Kaâniche · Eric Alata

Received: date / Accepted: date

Abstract This paper focuses on the security threats related to smart-TV communication channels. A risk analysis is carried out to have a global view of potential risks that need to be addressed in the context of Smart-TV communication links. The feasibility of several identified risks is investigated experimentally. The experiments show some relevant security-related vulnerabilities on Smart-TV communications channels. Countermeasures to address these vulnerabilities are also investigated.

Keywords Smart-TV · Risk Analysis · Security · DVB-T and Communication Channel

1 Introduction

Digital technologies have become widely used in home networks. At their beginning, the use of home Internet connections was mostly limited to provide access to the World Wide Web. More services have been provided later with the introduction of triple-play offers and the possibility to watch TV or initiate phone-calls using the Internet connection. The trend toward making every day home equipment "Smart"er has been strengthened over the past few years. As an example, kitchens are being equipped with smart-refrigerators, hospitalizations can be shortened by medical home equipment, and more and more domestic tasks can be supported by different smart automation systems. Many of these smart devices run operating systems and are connected to each other, through several networks, allowing them to interact and to be accessed remotely through the Internet. As a consequence, the security of such devices has become a real concern[13].

A typical example concerns smart-TVs. Besides receiving TV programs using an aerial antenna or a satellite dish, these new-generation TVs integrate an operating system running several applications and an internet connection, allowing them to offer more services to the users. Protocols, such as HbbTV[1], allow TV service providers to broadcast interactive Internet content simultaneously with their live TV shows. From a security point of view, two important aspects must be considered. Firstly, like any other embedded device, the embedded software may contain vulnerabilities that could be exploited by an attacker. Secondly, the simultaneous connectivity of the TV to several networks offer the opportunity to an attacker to use the TV as a gateway between these networks. Clearly, smart-TVs could represent a real security threat for home networks. Thus, it is important to carry out a global security analysis in order to identify potential threats and vulnerabilities and then investigate protection mechanisms to mitigate the related security risks.

To our knowledge, such a global security analysis has not been carried out so far. The first part of this expanded version of our article presented at the 45th annual IEEE/IFIP International conference on Dependable Systems and Networks (DSN 2015) [2] is aimed at filling this gap by studying the communication channels of a Smart-TV. EBIOS, an industrial risk analysis method developed by the French Network and Information Security Agency (ANSSI), is used to draw a global picture of the relevant risks, including those cited above, induced by the usage of smart-TVs in a home network. The second part describes the experiments we have carried out in order to illustrate the feasibility of attack scenarios corresponding to several vulnerabilities identified during the risk analysis.

We analyze in particular the security of two communication channels used by smart TVs: i) a bidirectional internet-based communication channel between the smart-TV and its service provider, and ii) a unidirectional communication channel for aerial TV broadcasts. The main lessons learned from our experiments concern 1) the fact that DVB broadcasts are not authenticated and are vulnerable to malicious attacks and

Y. Bachy
ISAE-SUPAERO
10, Avenue Edouard Belin
31400 Toulouse, France
E-mail: yann.bachy@isae-supaero.fr
+33 (0)5 61 33 80 84

V. Nicomette · Mohamed Kaniche · Eric Alata
LAAS-CNRS, Université de Toulouse, CNRS, INSA
Toulouse, France
E-mail: firstname.lastname@laas.fr

[1] Hybrid Broadcast Broadband TV

2) the fact that remote servers, such as software update servers, are not systematically authenticated and can be replaced by an illegitimate one using the ISP local loop. We have shown that it is possible to insert malicious traffic that could compromise the security of a smart TV, but also the security of other devices connected through the local network using the smart TV Internet connection. The last part of this paper discusses some countermeasures that could address the identified vulnerabilities.

This paper is structured as follows. Section 2 presents some related works that investigated different security issues of Smart-TVs. Section 3 presents the risk analysis we carried out, allowing us to get a global vision of the security threats smart-TV communication channels may be concerned by. More specifically, we explain how this risk analysis leads us to analyze the security of ADSL Internet connections and aerial DVB broadcasts. Then, Sections 4 and 5 present a set of experiments that allowed us to analyze the possible exploitation of some security related vulnerabilities discovered during the risk analysis. Then, Section 6 presents some countermeasures to cope with the risks we analyzed experimentally in this paper. Finally, Section 7 concludes and outlines some perspectives for future work.

2 Related works

In the coming few years almost 90% of the world-wide annually sold TVs will be smart-TVs [17] [10]. Moreover, many new smart-applications are taking profit of these smart-TVs in order to interact with the end-user. The popularity of these new-generation TVs makes them more and more attractive for attackers. This section gives an overview of some relevant vulnerabilities presented in related works, most often on newsgroups or technical blogs.

Many security issues often concern vulnerabilities where the end-users privacy is put in danger.

In [16], authors discuss an interesting feature of a specific Smart-TV which allows the user to control it's TV by voice commands. A quick analysis of the data sent out by the TV firstly shows that this feature is handled by a third party and secondly that the communication channel is not encrypted. This means any attacker, capable of intercepting data between the TV and the third party servers on the Internet is capable of listening to what is happening in the vicinity of the TV.

In [11] authors discuss how a specific smart-TV regularly sends viewing information about the programs watched regardless whether the specific `collection of watching info` option is switched on or off. Traffic analysis clearly indicates the smart-TV reports the channel being watched, and even worse, filenames stored on an external mass storage device, which could possibly contain sensitive private data.

In [14], the authors show that it is possible to determine the channel being watched based on statistical analysis determining the HbbTV page retrieved by the TV.

Other security issues exist. They often concern the possibility of impacting the integrity of smart-TVs.

In [21] authors study the possibility to modify the firmware of a Smart-TV, thereby impacting its integrity. Although the original firmware is encrypted using AES keys[2], the author was able to decode the firmware's content using tools provided by Altinyurt [1]. However, the author was unable to generate a modified firmware without a valid signature. Moreover, the author shows that it is possible to install some malicious widgets on the TV provided that the attacker has a physical access to the smart-TV in order to proceed with the installation of an unsigned application.

In [18], the authors were able to obtain a shell access on several smart-TVs by exploiting vulnerabilities in the smart-TV's multimedia player, without any physical access to the smart-TV. The wide usage of such integrated multimedia player could increase the likelihood of occurrence of such attacks.

In [3,4] the author studied possible attack scenarios through the service port located on the back of his smart-TV. The author initially showed that, thanks to 1) debug information captured at the service interface and 2) the exploitation of a network vulnerability (directory traversal), it is possible to extract the binary managing firmware updates. By analyzing this binary, the author was able to decode the firmwares of this TV and thereby analyze their content. At a second time, the author discovered the presence of a UPnP library containing a documented vulnerability. Thanks to all this information, the author was able to carry out a buffer overflow attack allowing him to activate a SSH server.

The following observations can be derived from the state of the art discussed above :

- All these studies address only one specific security issue individually;
- All the security issues pointed out use classical attack paths;

[2] Advanced Encryption Standard [9]

– Most of these published attacks target one specific TV brand at once.

More recent works point out new original attack paths which must also be considered. In [19] authors discuss the possibility to attack a smart-TV using data included in modern DVB-T TV broadcasts. This work has been technically validated in [2].

In this paper, a risk-analysis, based on the EBIOS method, is used in order to get a global view of potential risks that need to be addressed in the context of Smart-TV communication channels, without considering one particular brand or model. Our goal, on the first hand, is to identify new remote attack paths that can take benefit of the different communication interfaces of a Smart TV, and on the second hand, to develop an experimental testbed allowing us to investigate the feasibility of the identified attacks and to assess their potential impact. Relevant countermeasures to address such attacks are also investigated.

In the following section, we describe the risk analysis we have carried out on smart-TVs. We present the EBIOS methodology step by step, its application to smart-TVs and the conclusions we have derived from the analysis.

3 Risk analysis

Risk analysis methods address risk assessment and risk management. Many risk analysis methods exist (MEHARI (CLUSIF, 1997), OCTAVE (CERT, 1999), EBIOS (ANSSI, 1995),...). In our study, we used EBIOS as it has been developed by the French Network and Security Agency (ANSSI) and it is considered as a standard in France. Let us note the results of a Risk analysis are subjective according to the judgment of the analyst. However this can't affect the final results of the study.

This section is structured as follows. Firstly, we rapidly give an overview of the main activities carried out in the context of the EBIOS risk analysis method. Secondly, we present the results of the application of this method to smart-TVs and the relevant security related risks and threats that have been identified. Finally, possible counter-measures to mitigate these threats are discussed in Section 6.

3.1 EBIOS

Figure 1 presents the workflow defined by the EBIOS method. The risk analysis is decomposed into five main activities referred to as Modules. The first four modules are aimed at identifying and assessing relevant threats and associated risks, and the last module is dedicated to risk management.

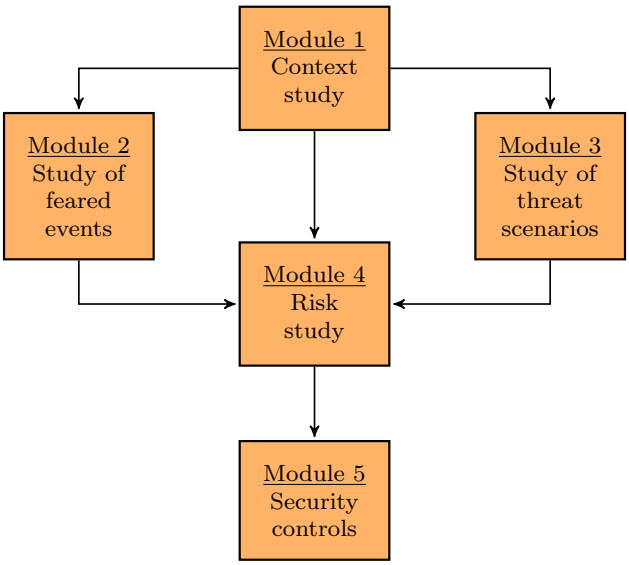


Fig. 1 The EBIOS method in 5 modules

Module 1, *Context Study*, consists in defining the context of the risk analysis. The results of the risk analysis highly depend on this definition as each context may not take into consideration the same user profile or point of view, and thereby may not have the same security needs. The context includes the definition of the different metrics that are used all along the study as well as the perimeter of the study. This module also defines the main assets and supporting assets (terms defined in EBIOS which we will discuss later) as well as existing security measures to be taken into account while defining security controls (Module 5). Modules 2 and 3, *Study of feared events* and *Study of threat scenarios* both contribute to the risk assessment. Module 2 defines the feared events by identifying the security requirements for each main asset as well as the impact in case these requirements are not met. It also defines the different possible sources of each threat. Module 3 identifies the potential scenarios that could lead to the feared events. Therefore, this module studies the threats that the sources could cause and exploitable vulnerabilities. Module 4, *Risk study*, confronts the feared events with the threat scenarios in order to obtain the different risks faced by the system. Module 5, *Security controls*, manages the risks identified previously by proposing countermeasures to be implemented.

In the rest of this section, we use the terms defined by the English version of the EBIOS method[3]. These

[3] `https://adullact.net/projects/ebios2010/`

terms are identified with the following font-type the first time they are used: `EBIOS term`.

In the following, we describe in more detail each module and present the results illustrating its application to the smart-TV case study.

3.2 Module 1: Context study

3.2.1 Objectives and boundaries of the study

The main goal of this study is to draw a global picture of the risks related to the usage of a smart-TV in a home environment. We consider a private usage of a smart-TV, and we adopt the point of view of the end-user. It is important to note that we do not focus on one particular smart-TV, instead we consider the general functions commonly implemented and used by most smart-TVs. Figure 2 illustrates a typical home network containing a Smart-TV with its multiple connections. In our use case we do not consider other devices on the local network in the house, that could also be compromised and perpetrate attacks on the Smart TV. We consider that such attacks are well-known and are thus out of the scope of this paper. In particular, two communication channels with the outside world are highlighted and explored in more detail in our study: 1) TV broadcasts though an aerial antenna or a satellite dish and 2) the local loop allowing the home network to be connected to the Internet.

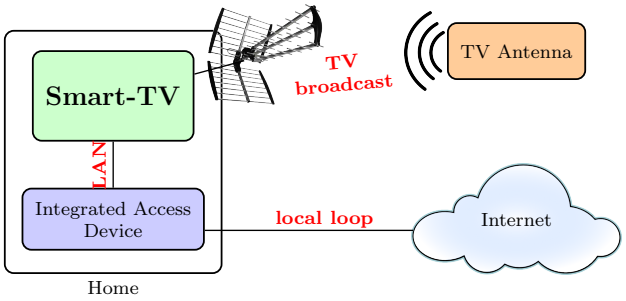


Fig. 2 Case Study: Smart-TV in a home network

In this context, we have identified nine threat sources presented in Table 1. In order to simplify the results of our study, we do not specify the capacities of each threat source. Indeed, EBIOS usually defines three capacity levels (`weak`, `important` and `unlimited`).

The "`Human`" column defines whether the source is human or not. For example, natural catastrophes or viruses don't need the immediate interaction of a human. The "`Int/Ext`" column localizes the source within the defined perimeter, in our case the user's home. The last column, "`Malicious`"[4], distinguishes malicious sources from accidental ones.

Table 1 Threat sources

Threat sources	Human	Int/Ext	Malicious
Malicious in-home user	✓	Int	✓
Clumsy in-home user	✓	Int	
Malicious outside person nearby	✓	Ext	✓
Malicious outside person	✓	Ext	✓
TV Operator	✓	Ext	
VoD Operator	✓	Ext	
TV Manufacturer	✓	Ext	
Virus[5]		Ext	✓
Weather problems		Ext	

5. Represents any malware spreading automatically.

3.2.2 Metrics definition

All along this study, we will be using different scales, which need to be defined. Indeed, each component of the studied system is evaluated according to several security `criteria`. These criteria correspond to the common security properties : Availability, Confidentiality and Integrity. In the context of this study we included the authenticity property also. For each one of these properties, it is necessary to define a scale for grading the importance of the expected `requirements`. The four criteria with their corresponding requirement levels are presented in Table 2. Let us note that these levels should correspond to the general needs and the tolerance of a user of the system. The EBIOS referential proposes standard scales on which are based the requirement levels we used in our study.

In EBIOS, risks are ranked according to their level of severity and their likelihood. In order to obtain this ranking, EBIOS combines the severity of each `feared event` and the likelihood of each `threat scenario` (these terms will be discussed later). The scales we used in our study to evaluate the severity and the likelihood are presented in Tables 3 and 4.

3.2.3 Asset identification

An EBIOS risk analysis decomposes the system into `main assets` and `supporting assets`. Main assets are defined as the informational patrimony or immaterial assets of the system which need to be protected. In our context, they are defined by identifying the main services delivered by the system. The supporting assets correspond to the different components supporting the implementation of the main assets. EBIOS defines nine pre-defined types of supporting assets:

[4] The EBIOS tool uses the term "malevolant", we prefer to use malicious.

Table 2 Security criteria

Availability		
Requirement		**Description**
1	More than 4h	Unavailability above 4h accepted
2	Between 1h and 4h	Unavailability between 1h and 4h accepted
3	Between 1m and 1h	Unavailability between 1m and 1h accepted
4	Less than 1m	Unavailability below 1m accepted

Integrity		
Requirement		**Description**
1	Acceptable	No need for integrity
2	Detectable	The alteration must be identifiable
3	Restrained	The alteration must be identified and corrected
4	Comply	The integrity must be enforced

Confidentiality		
Requirement		**Description**
1	Public	No need for confidentiality
2	Reserved	Accessible to a well defined limited group of persons or entities
3	Private	Accessible to one well defined specific person or entity

Authenticity		
Requirement		**Description**
1	Unknown	No need for authenticity
2	Identified	Identity declared, without guarantee of integrity
3	Authentic	Identity proven

Table 3 Severity scale

Level		**Description**
1	Negligible	No impact noticed
2	Limited	Minimal impact
3	Important	Severe but recoverable impact
4	Critical	Important impact, unrecoverable or with great difficulty

Table 4 Likelihood scale

Level		**Description**
1	Minimal	Once every 5 years
2	Significant	Once a year
3	Maximal	Daily

`premises`, `systems`, `hardware`, `software`, `networks`, `organizations`, `persons`, `papers` or `(interpersonal) channels`.

Considering our case study, we identified five main assets corresponding to the five main functionalities commonly provided by most smart-TVs:

- **Linear TV**: Television service where the viewer has to watch a scheduled TV program at the particular time its offered, and on the particular channel it's presented on. Hereinafter we only consider aerial connections, also known as terrestrial transmissions, which is the most used support over the world[8].
- **VoD**[6]: Service allowing the user to watch videos (movies, TV-shows, etc.) on demand.
- **PVR**[7]: Service allowing the user to record a linear TV-show on a physical storage device, such as a hard-drive for example.
- **Interactive TV (iTV)**: Service allowing the user to interact with a linear TV-show or to access other specific related content.
- **Network Media Player (NMP)**: Service allowing the user to watch multimedia content available through the local network and standard web-access.

One or several supporting assets are associated to each one of these main assets. In this study we selected a limited number of high-level supporting assets. If it reveals that more details are necessary, the analyst can either reiterate the risk analysis or conduct a new risk analysis on a specific sub-system. For this study we identified the following supporting assets:

- **Organization** *(ORG)*: TV operator, VoD provider.
- **Network** *(NET)*: Internet access, local area network, TV broadcast.
- **Software** *(SOF)*: Embedded software.

Table 5 presents the contribution of each supporting asset to the five main assets of the system.

Table 5 Relationships between supporting and main assets

	Main assets				
Supporting assets	**Linear TV**	**VoD**	**PVR**	**Interactive TV**	**NMP**
NET - Internet access		✓		✓	
NET - Local area network		✓		✓	✓
NET - TV broadcast	✓		✓	✓	
SOF - Embedded software	✓	✓	✓	✓	✓
ORG - TV operator	✓		✓	✓	
ORG - VoD provider		✓			

The last step of the context study is dedicated to the identification of existing security measures. These security measures may be specifically integrated in the device or should be available in the usual environment.

1. **Physical protection** offered by the premises (home) of the user against bad weather conditions but also against unauthorized physical access to the device. This allows to reduce the likelihood of physical attacks on the TV.
2. **Network Address Translation** offered by most home IADs[8] preventing devices, such as smart-TVs,

[6] Video on Demand

[7] Personal Video Recorder

[8] Most public internet providers include an Integrated Access Device (IAD) with their offer. These IADs have NAT activated by default.

connected to the local area network from being directly exposed to the Internet.
3. **Signed Firmwares** preventing man in the middle attacks from altering the embedded software and thus the behavior of a smart-TV.

This concludes the context study. We have now identified the main and supporting assets, existing security measures and the different security metrics for our study. The next two modules evaluate the security requirements and the impact in case these requirements are not respected.

3.3 Module 2: Study of feared events

Feared events are events during which a security requirement for a specific main asset is not fulfilled, for example: Linear TV availability. In other words, this module defines for each security criteria of each main asset:

- the expected security requirement,
- the possible sources of the threats that could prevent the system from fulfilling the expected requirement,
- the possible impacts in case a security requirement is not met, and
- the severity of the impact.

We defined the following impacts in the context of this study: Inactivity, No information (or incorrect information) displayed, Loss of private data[9], Financial loss and Activity disclosure.

The idea here, is to represent the requirements of an average domestic usage of a Smart-TV. Table 6 indicates the severity of the impact in case the security requirement of a main asset is not met.

Instead of discussing the detailed list of feared events resulting from the application of this approach to our smart-TV case study (which would be tedious), we focus on two particular feared events that will be detailed in the second part of this paper.

The two feared events that we considered as the most relevant ones and that will be the subject of the second part of this paper, are:

Linear TV - Authenticity
The feared event in this case corresponds to a malicious TV broadcast.

[9] We consider recordings made by the PVR just like any other private data stored on the Smart-TV.

Table 6 Severity of the impact in case a security requirement is not met

	Security criteria			
Main assets	**Availability**	**Integrity**	**Confidentiality**	**Authenticity**
Linear TV	Critical	Limited	Important	Important
VoD	Limited	Limited	Important	Limited
PVR	Negligible	Limited	Important	Limited
Interactive TV	Negligible	Limited	Important	Critical
NMP	Negligible	Limited	Important	Important

- Security requirement: The displayed information should be authentic (Apart from distraction, television is an important medium for the broadcast of official and possibly critical information.)
- Threat sources: malicious external person nearby home.
- Impacts: no information (or incorrect information is displayed).
- Severity: important (Although television can be used to inform the population, it is not the only medium used).

Interactive TV - Authenticity
This feared event corresponds to a modification of the data included in a TV broadcast allowing a TV set to interact with the TV channel which is being watched.

- Security requirement: The information displayed should be authentic (Interactive TV needs local code execution on the TV set, this code should not affect the security of the TV set).
- Threat sources: malicious external person nearby home, TV Operator, virus.
- Impacts: no information (or incorrect information displayed).
- Severity: critical (Interactive TV needs local code execution on the TV set, it is vital to be able to identify the source of this code.)

3.4 Module 3: Study of threat scenarios

This module consists in evaluating the likelihood of each threat scenario that corresponds to the failure of a specific security requirement for one supporting asset. Therefore, it requires to identify, for each security criteria, and for each supporting asset:

- the potential threat sources,
- the threats,
- the likelihood of the threat scenario occurrence.

Like in the previous module, instead of giving the detail for each "supporting asset / security criteria" combination, Table 7 indicates the occurrence likelihood of each threat scenario. We did not evaluate the

Table 7 Likelihood of threat scenario execution

Supporting assets	Availability	Integrity	Confidentiality	Authenticity
Internet access	Significant	Minimal	Minimal	Significant
Local area network	Minimal	Minimal	Minimal	Minimal
TV Broadcast	Minimal	Maximal	-	Significant
Embedded software	Minimal	Minimal	Significant	Significant
TV Operator	Minimal	Minimal	Significant	Significant
VoD Provider	Significant	Minimal	Significant	Significant

threat scenario concerning the confidentiality of a TV broadcast which makes no sense by definition. Let us focus on three examples:

TV Broadcast - Authenticity
This threat scenario corresponds to a malicious replacement of the TV broadcast channel used by the TV in order to receive the contents of TV channels.

- Threat sources: malicious person nearby home.
- Threats: data altered.
- Likelihood: Significant.

Internet Access - Authenticity
This threat scenario corresponds to a malicious replacement of the Internet channel used by the TV in order to access interactive services over the Internet.

- Threat sources: malicious person nearby home, virus.
- Threats: data altered, medium replaced.
- Likelihood: Significant.

Internet Access - Confidentiality
This threat scenarios corresponds to a disclosure of data sent or received by the smart-TV.

- Threat sources: malicious person nearby home, virus.
- Threats: data disclosed.
- Likelihood: minimal.

At this stage, we have identified the feared events and threat scenarios that are relevant to our smart-TV case study. The fourth module of EBIOS will combine these in order to define the associated risks.

3.5 Module 4: Risk study

This module consists in combining the data gathered during modules two and three in order to identify the risks that are relevant to the target system. The EBIOS method proposes two options to identify these risks.

The first method considers each threat scenario corresponding to each feared event individually.

Example: Network Media Player The availability of the Network Media Player can be affected by the unavailability of the local area network or the unavailability of the embedded software (cf. Table 5). When considering the other security criteria (cf. Table 2), we obtain the same relationships between threat scenario and feared events. Finally this method would lead to 8 risks for the Network Media Player as shown in Table 8.

Table 8 Risks for the network media player

	Security criteria			
Supporting assets	**Availability**	**Integrity**	**Confidentiality**	**Authenticity**
NET - Local area network	Risk 1	Risk 2	Risk 3	Risk 4
SOF - Embedded software	Risk 5	Risk 6	Risk 7	Risk 8

The second method only considers the feared events. Their likelihood is then calculated by determining the maximum likelihood of the corresponding threat scenarios.

Example: Network Media Player The authenticity of the Network Media Player is considered as one risk, thereby combining the impact of a non-authentic local area network and non-authentic embedded software. Considering the likelihood of these two threat scenarios are respectively Minimal and Significant, the likelihood of this risk is Significant. By applying the same approach for the other security criteria we obtain 4 risks for the Network Media Player.

For our case study, the first method leads to 60 risks. This would give a very detailed view to an analyst. The second method leads to 20 risks. This allows the analyst to obtain a global overview of all the risks the system is concerned by.

In this study we applied the second option, allowing us to obtain a "severity-likelihood" view of all the risks of our system. These risks are represented in Table 9.

Four different color zones are defined to distinguish the corresponding risk "level". In the following, we will focus on the threats belonging to the "red zone" which includes the risks for which severity is *Critical* and likelihood is *Significant or Maximal*, and those for which the severity is *Important* and the likelihood *Maximal*. This zone contains one risk:

Interactive TV non authentic *(iTV authenticity)*
Interactive TV is an application displaying interactive content on the TV screen[10]. The interactive content

[10] In this study we focus on the integrity of the interactive content and not the application processing this content.

Table 9 Risk analysis

	Likelihood		
Severity	Minimal	Significant	Maximal
Negligible	PVR availability NMP availability	iTV availability	
Limited	VoD integrity NMP integrity	VoD availability VoD authenticity PVR authenticity	TV integrity PVR integrity iTV integrity
Important		TV confidentiality TV authenticity VoD confidentiality PVR confidentiality iTV confidentiality NMP confidentiality NMP authenticity	
Critical	TV availability	iTV authenticity	

can be provided either through the TV broadcast, or through the Internet connection. This application is part of the embedded software[11] of the TV. This leads us to explore two different threat scenarios:

- **authenticity** of the TV broadcast, transporting the initial configuration of Interactive TV and in some cases the Interactive TV content. Therefore, we decided to analyze the security of a DVB broadcast reception.
- **authenticity** of the Internet access, through which software updates and in many cases the Interactive TV content are received. Therefore we decided to analyze the security of domestic Internet connections. These internet connections are composed of a series of different communication channels of which we will analyze the local loop.

Indeed, the TV broadcast and the local loop are two privileged networks between the service providers and the user, in the sense that each communication must transit over these communication channels. Moreover, these communication channels are easily identifiable, since they reach the user's home. To our knowledge, very few related works addressed the security analysis of these networks.

The next part of this paper is aimed at analyzing experimentally potential attacks related to these two threat scenarios and exploring possible countermeasures to face them. Firstly, the following section briefly presents some technical solutions: i) to observe the communication traffic between a smart-TV and a service provider, and ii) to simulate the behavior of a service provider and illustrate different examples of attack scenarios. The results are discussed in Section 5.

[11] Considering our study only focuses on communication channels we will hereinafter either use the term software or embedded software to refer to any software of a smart-TV

4 Experimental setup

This section describes the solutions we have used or developed in order to conduct our experiments. Some of these solutions are based on existing software, others require a specific hardware setup. These platforms allowed us to carry out some comparative studies which are presented in section 5. For each communication channel (ADSL local loop & DVB broadcast) studied, we proceed in two steps 1) analyze and understand the legitimate traffic and behavior of the network, and 2) simulate the service provider on the other side of the network, that interacts with the smart-TV.

4.1 ADSL local loop

The first study that we have carried out focuses on the analysis of the local loop supporting the ADSL network. This network was historically installed for public switched telephone networks (PSTNs). Besides telephony, this network now transports other services such as Internet and TV. This implies that many data communications, possibly critical, use this network.

There are 4 main physical supports used for the local loop: copper pair, coaxial, fiber optics and radio waves. We hereinafter only consider copper pair local loops. The method developed in our study can be applied to any kind of local loop by using analogous hardware. This copper pair is terminated by a MoDem (*Modulator and Demodulator*) on the user's side, and by a DSLAM (*Digital Subscriber Line Access Multiplexer*) on the Internet provider's side. These two equipments modulate and de-modulate a digital signal into

analog signals which are transmitted over the copper pair.

4.1.1 Traffic observation setup

This setup is intended to observe any traffic on a copper pair local loop and is composed of a DSLAM and an ADSL modem.

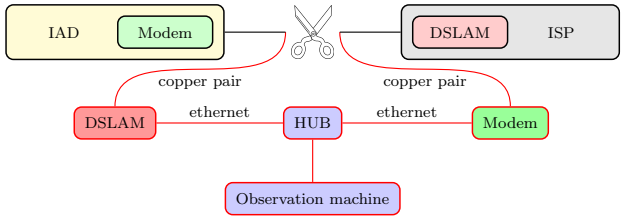


Fig. 3 Local loop traffic capturing

The DSLAM and modem at each end of the copper pair fulfill the exact opposite operation of each other. Indeed, the modulation used on the up-stream differs from the one used on the down-stream. Therefore, it is possible to physically cut the line and insert a new DSLAM and a new ADSL modem, while preserving the connectivity between the customer and the Internet service provider. In fact, this modification changes the way the IAD communicates with the provider's DSLAM: it synchronizes and communicates with the inserted DSLAM; the inserted DSLAM communicates with the inserted ADSL modem which, in turn, synchronizes and communicates with the provider's DSLAM. As the local network interface included in both modems and DSLAM is most of the time Ethernet, this setup finally consists in transforming one copper line into two copper lines interconnected by an Ethernet LAN (see Figure 3). As sniffing Ethernet LAN traffic is very easy, the communications sent and received by the IAD, or any other smart-device connected to the home network, can be observed.

4.1.2 Service provider simulation setup

This platform simulates a service provider based on the knowledge of our target system acquired using the traffic observation platform or other reverse engineering techniques. Here, instead of connecting the inserted DSLAM to the provider's network using a modem, we connect it to a computer capable of simulating the behavior of the Internet service provider, which in turn is connected to a second computer capable of simulating the service provider of our target system (cf. Figure 4). The installation of these servers is accomplished step by step following an iterative method. We cyclically reboot the target system (IAD for the ISP simulator, Smart-TV for the Online Service Simulator), observe any request coming from the target system and answer it by installing corresponding software based on the knowledge we have of the target system.

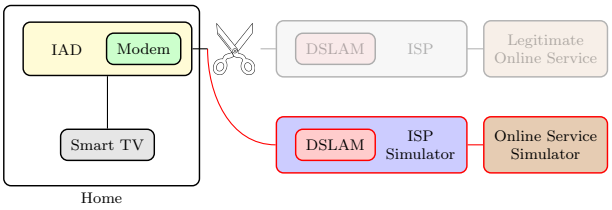


Fig. 4 Simulating an online service

4.2 DVB Broadcasts

The second service provider network we have tested is the aerial DVB-T system used for digital Television. TV broadcasts are generally considered as trustworthy. Traditional television is based on only one unidirectional communication system, which implies that consumers do not have to worry about privacy. With Digital TV and smart-TVs, even though DVB-T is still a unidirectional communication channel, it is not the only mean of communication: TV broadcasts tend to take benefit of the internet access to propose more interactive content. Therefore previous assumptions are no longer valid, which makes it relevant to analyze the security of smart-TV communication channels. DVB Broadcast security concerns have already been investigated[19] using some relevant aspects of modern Smart-TVs. However, to our knowledge there is a lack of experimental studies aimed at exploring possible attack paths and scenarios exploiting the new functionalities and services implemented in smart TVs. We hereinafter present the solutions we have used to conduct some comparative studies on different types of smart-TVs available on the market.

4.2.1 DVB

DVB is a suite of standards for digital television transmission[22]. It allows transmission of MPEG-2 Transport Streams, containing multiple video, audio or data streams, over several supports such as satellite, aerial or cable connections. Hereinafter we only consider aerial connections, also known as terrestrial transmissions, which is the most used support over the world[8]. Such aerial transmissions are terminated by a DVB-T demodulator at the user's side, and by a DVB-T modulator at the provider's side.

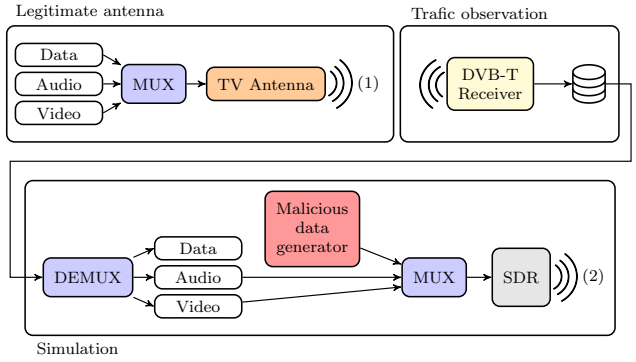


Fig. 5 DVB Experimentation platform

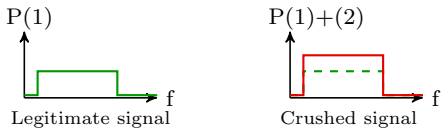


Fig. 6 Signal crushing

4.2.2 Traffic observation setup

The objective is to observe every stream received by a TV tuned into a specific frequency. As listening to a DVB-T broadcast signal is implemented by any TV, this solution does not require any specific hardware. Any off the shelf DVB-T demodulator can be used. Open-source software such as DVBSnoop[12] allows DVB MPEG stream analysis. We use tzap software[13] to tune the demodulator into the target frequency.

4.2.3 DVB Broadcast simulation solution

This solution is intended to simulate a legitimate DVB broadcast. In order to broadcast a valid DVB channel, we need a DVB valid MPEG TS and a DVB-T modulator. Many popular open-source applications such as ffmpeg[14] and vlc[15], are capable of generating and modulating MPEG TSs. However, these applications cannot be used to obtain a DVB valid MPEG TS as they are not able to create DVB-required signaling tables. This can be achieved by the opensource application: Avalpa OpenCaster[16]. This task can be initiated by capturing a legitimate signal (cf. Figure 5 - traffic observation).

Since broadcasting TV without a license is prohibited in most countries, DVB modulators are generally not available off-the-shelf. During our experiments, we have used two solutions. The first one uses hardware suggested by OpenCaster, which can be purchased online. This DVB modulator functions "out-of-the-box" with OpenCaster, but is limited in some modulation parameters, i.e., it only supports QPSK or QAM16 constellations, considerably reducing the available bandwidth. Since many countries use the QAM64 constellation, this hardware is unable to entirely simulate a DVB Multiplex. The second platform we have experimented requires more expensive SDR (Software Defined Radio) hardware. In our case, we used the Ettus N210 with the WBX daughterboard. Using GNU-Radio[17] makes it possible to turn such a device into any kind of radio modulator, including a DVB-T modulator. The popularity of GNU-Radio allowed us to find an entire DVB-T modulation scheme[5] online. Combining one of these two hardware solutions with OpenCaster allowed us to set up a fully functional DVB-T modulator (cf. Figure 5 - simulation).

When considering wired networks, physically connecting the end user to the simulation platform forces the end users terminal to communicate with this platform. In our case, using an aerial transmission, one cannot just plug out the legitimate service provider and plug in our simulation platform instead. We need to crush the legitimate signal, which can be done by transmitting with significantly more power or by approaching the victim's antenna in such a way that our signal will be perceived as being significantly stronger than the legitimate signal. The International Telecommunication Union defines [15] safety ratios, to make sure a weaker signal won't interfere. Thus, if one transmits above these safety ratios, the emitted signal crushes the legitimate one, and any TV around considers this signal rather than the legitimate one (cf. Figure 6).

It is important to note that we did not carry out large-scale experiments. Instead, we limited our experiments to our research lab, making sure that our experiments did not interfere with any legitimate signal.

5 Experimental results

We used the traffic observation and service provider simulation platforms described in Section 4 to carry out several experiments on a panel of four main-brand

[12] http://dvbsnoop.sourceforge.net/
[13] http://www.linuxtv.org/wiki/index.php/LinuxTV_dvb-apps
[14] https://www.ffmpeg.org/
[15] http://www.videolan.org/vlc/
[16] http://www.avalpa.com/the-key-values/15-free-software/33-opencaster
[17] http://gnuradio.org/

mid-range Smart-TVs, which were the most sold smart-TVs in Europe for 2013, and are therefore representative of the average domestic smart-TV. All have an Ethernet connection and implement a "smart" environment including standard applications such as a Web-Browser and VoD. Hereinafter, these TVs are anonymously referenced as A, B, C and D.

The first set of experiments uses the local loop setups in order to analyze and compare the communication protocols used between a Smart-TV and different online services, and their configuration. As the embedded software of a smart-TV is a very critical element, a first experiment focuses on potential vulnerabilities and potential attacks targeting the procedure used for updating embedded software. Hereby we address one of the most important threat scenarios addressing the risks related to integrity problems.

A second experiment focuses on the smart-TV's integrated Web browser and its compliance to the same-origin security policy[18]. Hereby we address another important threat scenario, that could affect the integrity of smart-TVs and other devices connected to the same computer network.

The second set of experiments uses our DVB Broadcasting platforms, allowing us to analyze and compare the behavior of each Smart-TV when receiving legitimate and compromised TV signals. A first experiment shows an interesting way of compromising a DVB-T Broadcast. Hereby we address threat scenarios related to linear and interactive TV authenticity risks.

A second experiment analyzes again the compliance to the same-origin security policy, but now using the embedded HbbTV browser.

The result of this last experiment allowed us to illustrate a combined attack scenario, compromising a home network due to lack of security in Smart-TVs and their respective networks.

Table 10 summarizes the experiments that we have carried out considering local loop and DVB broadcast attacks. The results are detailed in the following subsections.

[18] The same-origin security policy defines that the local execution of a code (i.e. javascript), downloaded from a remote Web site, cannot send data to a Web site who's origin (URL) differs from the one of the original Web site.

Table 10 Experiments summary

	1^{st} experiment	**2^{nd} experiment**
Local loop Setup	Software update procedure analysis	Web-Browser & same-origin policy
DVB Setup	DVB Broadcast authentication	HbbTV Browser & same-origin policy

5.1 Local loop experiments

The first two experiments are carried out using our local loop observation and service provider simulation platforms. These experiments could easily have been carried out on the local area network if the attacker was inside the target home. By operating on the local loop, these experiments demonstrate the possibility to remotely compromise someone else's TV. Indeed, operating directly on the copper pair local loop is technically more complicated as it requires a specific hardware setup but it presents a higher security impact, as it possibly allows to compromise any home. The two experiments we have choses only serve as an example, and we can imagine many more attacks using this attack vector.

5.1.1 Smart-TV software update procedures

The first experiment carried out on our panel of smart-TVs intends to analyze whether the communications during a software update procedure are protected. Our local loop observation platform (cf. Section 4.1.1) was placed behind the IAD, allowing us to observe any communication between the smart-TV and its online service provider[19]. The results of this experiment are presented in Table 11.

Table 11 Smart-TV software update procedures

Smart-TV		*A*	*B*	*C*	*D*
Negotiation	protocol	HTTP	HTTP + HTTPS	HTTPS	HTTP
	content	unknown	XML + *unknown*	*unknown*	XML
Transfer	protocol	HTTP	*unknown*	HTTP	HTTP
	content	Binary	*unknown*	Binary	Binary

In each software update procedure, two phases are distinguished. First, a "negotiation" phase that checks if a more recent software version is available for this Smart-TV. Secondly, if a newer version is available, a "transfer" phase wherein the actual software is transferred. For each phase, we observed the protocols that are used, and the type of content. Negotiation phases

[19] In this particular case, the online service provider of a smart-TV is considered as the servers belonging to the manufacturer of the TV and proposing software updates.

of A, B and C are very similar, they either use the secured HTTPS protocol, in which case the content is ciphered, or, when a non-secured protocol such as HTTP is used, the content uses an unknown encoding and can therefore also be considered as ciphered. The negotiation phase of D uses the non-secured HTTP protocol and its content is human readable XML. This allows a classic "man-in-the-middle" attack to substitute the URL leading to the new software and force the TV to download a different software.
All observed software transfer phases use the non-secured HTTP protocol, we were unable to observe the transfer phase for TV B. For each of these TVs, we carried out a "man-in-the-middle" attack simulating the update server during this phase, proposing legitimate but outdated software[20]. Smart-TVs A and C refused our outdated software without specifying any reason. It is likely that an anti-rollback mechanism is used. Smart-TV D on the contrary accepted our outdated software. This security breach allows any attacker to exploit any previously corrected security flaws on this TV.

5.1.2 Smart-TVs and the same-origin security policy

The second experiment on our panel of smart-TVs is an experience we carried out on both the local loop and the DVB-T broadcast. On the DVB-T broadcast the results of this experiment are siginifcant for our final combined attack (cf. Section 5.2.3). In this section we show how this attack vector also functions from the local loop.

This experiment intends to verify the compliance of the integrated Web browser of each Smart-TV to the same-origin security policy. During this experiment, we connected each TV to our ISP simulator (cf. Section 4.1.2). On our online service simulator, we hosted a Web site containing malicious JavaScript code containing a CSRF[21] attack. This JavaScript simply attempts to perform a HTTP POST request on a different[22] Web site. When a Web browser fully complies to the same-origin security policy, it must either first send out an "OPTIONS" request, as shown in fig. 7, or in the worst case simply ignore the request.

Table 12 reports the behavior of our four Smart-TVs. A, B and C are compliant to the same-origin security policy. D does not implement this security policy and sends out the malicious POST request. This security breach can be exploited by any phishing attack,

[20] We downloaded and archived legitimate software from the manufacturer's Web-sites.
[21] Cross Site Request Forgery, attacks that should be prevented by the same-origin policy.
[22] In XSS, we consider a different Web site as one having a different Fully Qualified Domain Name (FQDN).

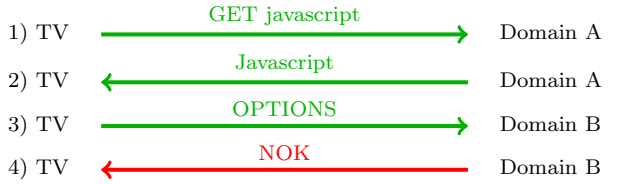


Fig. 7 Same-origin security compliant browser

Table 12 Smart-TV web browser and the same-origin policy

TV	*A*	*B*	*C*	*D*
Behaviour	Ignore	OPTIONS	OPTIONS	POST

i.e., by imitating a popular Web site. In section 5.2.2 we will compare these results when testing HbbTV.

5.2 DVB broadcast experiments

This set of experiments was carried out using our DVB observation and broadcast simulation platforms. They are aimed at investigating if the content of a TV channel is authenticated by a TV set.

DVB basically consists in broadcasting an MPEG Transport Stream (TS) flow, which is a multiplex of multiple Video, Audio and Data streams. DVB stipulates[20] that an MPEG TS can contain multiple channels of different quality. Oren and Keromytis [19] propose a solution to compromise a stream at real-time that requires directional antennas (cf. Section 4.2.3). Our solution requires less hardware. Our experiments use a pre-recorded part of the target multiplex. We then use the same technique to modify the content of a substream in the multiplex. The effect of the modification will be percieved by the end user who will notice a flashback in the TV program he is watching.

5.2.1 Compromising a DVB Broadcast

This first experiment intends to demonstrate that the content of a DVB Broadcast is not authenticated and that all our TVs correctly implement DVB specifications. In this experiment, we replace one of the video streams by a live webcam video feed. All the TVs of the test-panel ignore the legitimate signal when our platform is activated, and instead, show the live webcam feed. This experiment is achieved by recording a short duration of a legitimate DVB broadcast. Using our platform, we extracted one of the video streams out of the multiplex and then inserted our own video source instead. We obtained the same results when altering audio or specific data streams in our DVB multiplex.

5.2.2 HbbTV and the same-origin security policy

Similarly to the experiment described in subsection 5.1.2, we tested the same-origin security policy compliance using the HbbTV protocol. HbbTV allows DVB to include Internet content in a multiplex, either by multiplexing the entire Web page into the broadcast, or by providing the URL allowing the smart-TV to access the Web page using its Internet connection. Same-origin policy issues are discussed in [19], where authors are concerned about the possibility to define the origin when the Web page is entirely multiplexed into the broadcast. In this case, no origin is defined and a specific property, `simple_application_boundary_descriptor`[12, S6.3] allows the malicious broadcaster to define its own origin. We tested the same-origin security policy on our 4 smart-TVs with and without specifying this property. The results of these experiments are reported in Table 13.

Table 13 Smart-TV HbbTV and the same-origin policy

`boundary descriptor`	*A*	*B*	*C*	*D*
With	POST	Ignore	OPTIONS	OPTIONS
Without	POST	Ignore	OPTIONS	OPTIONS

These results are surprising and point out some interesting facts. First, there is no difference whether the `simple_application_boundary_descriptor` property is defined or not. This can be explained by the TV introducing a FQDN[23] when the Web page is embedded in the DVB broadcast, this FQDN appears in the origin headers as `dvb://1.1.1.b`. Therefore the `simple_application_boundary_descriptor` property is ignored because the application boundary can only contain one FQDN[12, S6.3]. Secondly, in comparison with the results of the experiments carried out in Section 5.1.2, where the Web browser of A would respect the same origin security policy by ignoring the CSRF attack, it now accepts to execute the attack and thereby ignores the security policy. On the other hand, D now fully respects the same-origin security policy while it did not in our previous experiment. Also B, even though it still complies with the security policy, behaves differently by ignoring the attack. This could mean that at least A, B and D don't use the same rendering software engine for the normal Web browser as for HbbTV. We exploited this security flaw on TV A by multiplexing a Web page, containing malicious JavaScript, directly into our malicious DVB signal[24]. This JavaScript code sends out a UPNP request to the local IAD, asking it to open specific ports to TV A. Doing so allowed us to conduct attacks which were, up to now, only feasible from the local area network.

5.2.3 Combined attack

Many related works discussed in Section 2 present specific vulnerabilities on different smart-TVs. Even if the exploitation of such vulnerabilities is particularly interesting for an attacker, their scope is often limited, due to massive use of NAT techniques on home networks. The usage of NAT limits direct access from the Internet to devices connected through a local area network. Therefore these attacks can only be executed from machines connected to the LAN, i.e, from inside the house. The scope and the scale of these attacks may drastically change if they could be carried out from outside the house, i.e., from the Internet. This could be possible with the novel attack path described in Section 5.2.2. Indeed, in this section, we presented a first exploitation on a smart-TV using an attack path combining the usage of a DVB broadcast and a home Internet connection. One part of this attack consisted in forging a UPNP request asking the local IAD to open a specific port to the target device, as explained in the previous section.

As an example, we forged a UPNP request in order to open the port corresponding to a web service available on one of our smart-TVs, that allows to control the TV like a remote control. In most use-cases, this web service is only accessible from the local area network. By carrying out our attack, we are now able to change the volume and channel of the TV over the Internet. In other words, this means that, by carrying out this attack, an attacker is able to change the volume and channel of any Smart TV of his choice, from the Internet. In the same way, attacks described in Section 2, requiring an access to the local network, also become possible from the internet.

At a larger scale, this operation can be repeated in order to open any other port. If we repeat this operation until we have opened all the available services on a smart-TV to the Internet, the TV is no longer protected by NAT. Any attack[25] which would up to now require a direct access to the local area network, become fully functional through the Internet. This means that

[23] Fully Qualified Domain Name

[24] This attack can be achieved either by including the JavaScript in a data carousel multiplexed into the DVB signal, or by supplying an URL pointing to an external Web page containing this malicious code.

[25] Attacks requiring broadcast packages will not function over the Internet.

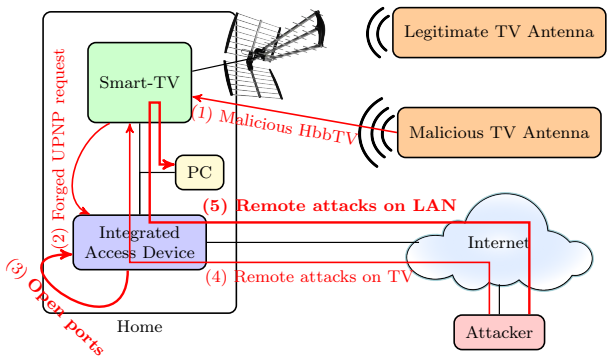


Fig. 8 Combined attack

thanks to our attack path, many vulnerabilities could be exploited remotely on a TV.

From there on, it is possible to imagine any kind of attack on a home network. Indeed, once the attacker gains control over the TV, he may use it as a gateway in order to exploit vulnerabilities in any other smart device inside the home. As a consequence, the corruption of a Smart TV from the Internet may possibly endanger any other device connected to the home network. This combined attack is described step by step in figure 8.

6 Countermeasures

The last module of the EBIOS method is dedicated to security controls, in other words, the definition of countermeasures to mitigate the risks identified during the risk analysis. Considering the experiments discussed in the previous sections, the attack scenarios that we have identified are mainly related to: i) a lack of protection of the communication channels, combined with ii) a lack of enforcement of the same origin security policy by the web-browsers involved in the interaction between the smart-Tv and the service provider.

In this paper, we analyzed the security of two typical communication channels used by smart-TVs: i) a bidirectional internet based-communication between the Smart-TV and its online service provider, and ii) a unidirectional communication for the aerial broadcast.

More generally, the problems raised are very similar for any Internet connected device. During our experiments we have noticed that the different communication channels used by a smart-TV, and especially those communicating with their service providers do not always implement sufficient security measures, in particular to enforce protection against authenticity attacks. More generally, each smart-device has n communication interfaces[26] allowing data transmission to or reception from another entity. Globally, for each link, and for each security property[27], the needs should be analyzed. Hence, each security criteria is not systematically required on each communication channel and must be studied individually.

By identifying the needs on each communication channel it is possible to determine the corresponding security measures. Several security methods exist on different layers of the OSI model. For classic Internet communication channels, most standard security measures are well-known and mature. For example, usage of TLS on layer 4, IPSec on layer 3 or VPN tunnels on either layers 3 and 4. Indeed, during our experiments we have observed several devices integrating sufficient and well configured security mechanisms on the Internet communication channels. In most cases TLS is implemented at the transport layer, and in some cases a specific security mechanism is implemented at the application layer. In either case, we consider these mechanisms are well known and do not need to be discussed further, although we do consider their usage should be more systematic. Considering aerial broadcast communications, to the best of our knowledge, security protection mechanisms have been seldom addressed. Therefore, the rest of this section discusses existing security mechanisms for DVB broadcasts. We firstly present the protocol stack of an aerial TV broadcast, before identifying the different security mechanisms for each layer of this stack.

6.1 DVB protocol stack

In most cases, TV channels are transmitted on a one-way communication channel. Since broadcasting on frequencies reserved to television broadcasts, without a license, is forbidden in most countries, the definition of the protocols used, is often less detailed. However, the experience acquired during our experiments, allowed us to distinguish 3 layers presented in Figure 9.

6.2 The higher layers

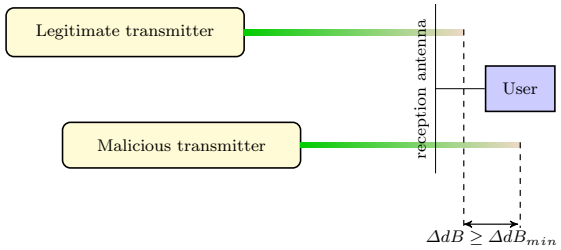
The higher layers of the DVB stack are independent of the physical medium used. Therefore, the security

[26] We distinguish 5 main types of communication interfaces: human-machine (Keyboard, Screen), Peripheral (USB, Firewire, WigBee), Remote service (DVB, PSTN), Internet (xDSL, RJ45, Wifi, 3G) and Manufacturer (RS232, JTAG).

[27] Availability, Integrity and Confidentiality, by extension, the integrity of meta-data makes us consider Authenticity aspects also.

No	No OSI	Name	Description
3	5-7	Application	Multimedia streams & data
2	4	Transport	DVB Multiplex
1	1-3	Physical	Definition of physical transmission properties

Fig. 9 DVB stack



ΔdB_{min} = threshold defined by the protocol.

Fig. 10 Power difference of the received signal

measures of these layers are identical for the different DVB modes (DVB-S, DVB-C, DVB-T, ...).

On the higher layers only two security mechanisms exist. The first mechanism to be considered is digital right management (DRM) for MPEG streams [6,7]. However, this mechanism doesn't offer any protection in terms of communication integrity or authenticity for the end-user.

The second mechanism is directly related to Pay-TV for which DVB uses the common scrambling algorithm (CSA) [23]. This mechanism offers an access control mechanism for pay-TV providers, using a symmetric encryption mechanism. The encryption key is transmitted together with the encrypted content, protected by an asymmetric encryption mechanism. The user has a smart card, capable of decrypting the encryption key that is used to decrypt the TV channel. It is impossible for an attacker to replace an encrypted stream by its own encrypted stream. Therefore, an attacker would need to access a DVB-CSA3 encryption device, which isn't freely available.

6.3 The lower layers

The lower layers of a DVB broadcast depend on the transport medium used. Considering DVB-T, used for terrestrial aerial transmissions, the International Telecommunications Union [15] defined thresholds in order to avoid signal interference. This means that, for an attack to succeed, the receiver must receive a stronger signal during the attack. This can either be achieved by increasing the transmission power, or by approaching the malicious transmitter. This situation is presented in Figure 10.

The smart-TV could then alert the user if an abnormal situation is detected. This mechanism can only function on relatively stable aerial transmissions. Indeed, in situations where at least one of the two entities of the communications constantly moves, such as with mobile phones, such measures are not relevant.

6.4 Summary

From a security point of view, it is essential to improve the DVB standards in order to integrate security mechanisms capable of guaranteeing the authenticity of communication data inside a DVB broadcast. Such a mechanism could be similar to the way an Internet browser functions, by validating the certificate of the transmitter in a trusted list. This concept could be extended by regularly including a signed checksum of the entire multiplex, allowing a TV set to check the authenticity of the entire DVB broadcast.

7 Conclusion

In this paper, we have first presented our application of the EBIOS risk analysis method on smart-TVs. This analysis allowed us to obtain a global vision of the main risks any smart-TV may be concerned by. In the second part of this paper, we carried out several experiments, in order to check the feasibility of a new attack path that allows remote vulnerability exploitation on Smart devices in a home network. This new attack path was instantiated on a panel of different types of commercially available Smart TVs. Our experiments allowed us to successfully 1) modify the software of some models of Smart TVs and 2) exploit a cross-site vulnerability in HbbTV browsers of some models, which in turn can be used to modify the UPNP configuration of the home network IAD, opening a new remote access from the Internet to the Smart TV. Finally, in the last part of this paper, we studied some possible countermeasures to the different weaknesses identified during these works.

During our experiments we have observed that most standard IP communications are well protected. Indeed, many Smart-TV manufacturers already use the secure HTTPS protocol or other proprietary protection mechanisms (encryption, signature, anti-rollback mechanism) in order to secure their software update process. However, we have noticed that security is less well integrated on other communication channels. In our case,

it was easy to compromise the DVB broadcast communication. This communication should no longer be ignored when considering the overall security of Smart-TVs.

As future work, we plan to further investigate how an attack, issued from a DVB network and targeting a Smart TV, could propagate on the home network, and in turn target other devices connected to this LAN. We plan to conduct experiments aiming at building a generic home network, including several connected devices and analyzing these attack propagation possibilities. This research topic is not specifically limited to Smart TVs, and we plan to address this issue globally, taking into account various families of connected devices and all their network connections.

References

1. Altinyurt, E.U.: Samygo. http://www.samygo.tv. (visited on 2015-04-28)
2. Bachy, Y., Basse, F., Nicomette, V., Alata, E., Kaâniche, M., Courrege, J.C., Lukjanenko, P.: Smart-tv security analysis: practical experiments. In: Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Conference on, pp. 497–504. IEEE (2015)
3. Basse, F.: Sécurité des ordivisions. In: proc. of Symposium sur la sécurité des technologies de l'information et des communications (SSTIC). Rennes, France (2014)
4. Basse, F.: Télévisions connectées : Des objets branchés sécurité ? Multi-System and Internet Security Cookbook (MISC) (2014)
5. Bogdan: Dvb-t implementation in gnuradio? part 2. http://yo3iiu.ro/blog/?p=1220. (visited on 2015-04-28)
6. Chen-Wei, F., Feng-Cheng, C., Hsueh-Ming, H.: An MPEG-4 IPMPX design and implementation on MPEG-21 test bed. In: International Symposium on Circuits and Systems, 2005. ISCAS 2005., pp. 4550–4553 Vol. 5 (2005). DOI 10.1109/ISCAS.2005.1465644
7. Cho, Y., Seok, J., Hong, J., Ahn, C.: Broadcasting system compliant with MPEG-2/4 IPMPX. Electronics and Telecommunications Research Institute journal (ETRI) **26**(2), 83–91 (2004)
8. Commission, E.: Special eurobarometer 438: E-communications and the digital single market. https://data.europa.eu/euodp/en/data/dataset/S2062_84_2_438_ENG (2016). (visited on 2017-09-11)
9. Daemen, J., Rijmen, V.: The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media (2002)
10. digitaltveurope.net: Smart tv sales boost overall european market. http://www.digitaltveurope.net/349582/smart-tv-sales-boost-overall-european-market/ (2015). (visited on 2015-10-02)
11. DoctorBeet: Lg smart tvs logging usb filenames and viewing info to lg servers. http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html (2013). (visited on 2015-04-28)
12. European Broadcasting Union: ETSI TS 102 796 V1.2.1 (November 2012)
13. Feamster, N.: Outsourcing home network security. In: Proceedings of the 2010 ACM SIGCOMM Workshop on Home Networks, HomeNets '10, pp. 37–42. ACM, New York, NY, USA (2010). DOI 10.1145/1851307.1851317. URL http://doi.acm.org/10.1145/1851307.1851317
14. Ghiglieri, M., Tews, E.: A privacy protection system for hbbtv in smart tvs. In: Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, pp. 357–362 (2014). DOI 10.1109/CCNC.2014.6866595
15. International Telecommunication Union: Planning criteria, including protection ratios, for digital terrestrial television services in the vhf/uhf bands (2014)
16. Lodge, D.: Is your samsung tv listening to you? http://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/?_ga=1.198058351.1988843124.1443693594 (2015). (visited on 2015-10-01)
17. van der Meulen, R., Rivera, J.: Gartner predicts live video broadcasting will be the new "selfie" by 2017. http://www.gartner.com/newsroom/id/2934717 (2014). (visited on 2015-10-02)
18. Michele, B., Karpow, A.: Watch and be watched: Compromising all smart tv generations. In: Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, pp. 351–356 (2014). DOI 10.1109/CCNC.2014.6866594
19. Oren, Y., Keromytis, A.D.: From the aether to the ethernet—attacking the internet using broadcast digital television. In: 23rd USENIX Security Symposium (USENIX Security 14), pp. 353–368. USENIX Association, San Diego, CA (2014). URL https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/oren
20. Reimers, U.: The dvb project-digital television for europe. In: DVB (Digital Video Broadcasting): The Future for Television Broadcasting?), IEE Colloquium on (Digest No.1995/142), pp. 1/1–1/7 (1995). DOI 10.1049/ic:19950880
21. Sidiropoulos, N., Stefopoulos, P.: Smart tv hacking. In: Research project 1. Amsterdam, Netherlands (2013). URL http://delaat.net/rp/2012-2013/p39/report.pdf
22. Stott, J.: The dvb terrestrial (dvb-t) specification and its implementation in a practical modem. In: Broadcasting Convention, International (Conf. Publ. No. 428), pp. 255–260 (1996). DOI 10.1049/cp:19960816
23. Weinmann, R.P., Wirt, K.: Communications and Multimedia Security: 8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Sept. 15–18, 2004, Windermere, The Lake District, United Kingdom, chap. Analysis of the DVB Common Scrambling Algorithm, pp. 195–207. Springer US, Boston, MA (2005). DOI 10.1007/0-387-24486-7_15. URL http://dx.doi.org/10.1007/0-387-24486-7_15