Protocole HbbTV et sécurité : quelques expérimentations

Yann Bachy, Vincent Nicomette, Eric Alata, Mohamed Kaâniche,
Jean-Christophe Courrège, Pierre Lukjanenko

Protocole HbbTV et sécurité : quelques expérimentations

Yann Bachy[1,2,4], Vincent Nicomette[1,2], Eric Alata[1,2], Mohamed Kaâniche[1,3], Jean-Christophe Courrège[4] et Pierre Lukjanenko[1]
[1] prénom.nom@laas.fr
[4] prénom.nom@thalesgroup.com

[1]CNRS, LAAS, 7 Avenue du colonel Roche, F-31400 Toulouse, France
[2] Univ de Toulouse, INSA de Toulouse, LAAS F-31400 Toulouse, France
[3] Univ de Toulouse, LAAS, LAAS F-31400 Toulouse, France
[4] Thales Communications & Security, 3, avenue de l'Europe, 31400 Toulouse, France

Résumé Les smart-TVs sont de plus en plus présentes dans nos domiciles. Au même titre que les différents objets connectés qui envahissent notre quotidien professionnel et familial, ces téléviseurs de nouvelle génération, embarquent un système d'exploitation, pouvant contenir des vulnérabilités susceptibles d'être exploitées par des attaquants. Le but de cet article est d'étudier ces vulnérabilités, et en particulier celles qui sont liées à l'utilisation du standard DVB (*Digital Video Broadcasting*) et du protocole HbbTV (*Hybrid Broadband Broadcast TV*). Cet article présente des expérimentations qui nous ont permis, d'une part, de montrer que les téléviseurs n'authentifient pas l'émetteur des flux DVB qu'ils reçoivent, mais également d'exploiter des vulnérabilités des téléviseurs à l'aide de données spécifiquement incluses dans ces flux.

1 Introduction

Les technologies numériques envahissent de plus en plus notre quotidien, à la fois professionnel et familial, et permettent d'accéder à de plus en plus de services. A titre d'exemple, nos lecteurs DVDs, nos téléviseurs, nos systèmes d'alarmes, même nos réfrigérateurs peuvent être aujourd'hui connectés au réseau Internet. Ces objets connectés sont des systèmes informatiques, puisqu'ils exécutent un système d'exploitation, aussi appelé *firmware*. Ce système implémente de multiples protocoles de communication, permettant à l'objet de se connecter au réseau Internet mais aussi de communiquer avec d'autres objets. Comme pour tout système informatique, on peut s'interroger sur la sécurité de ces équipements [10]. L'ANSSI [2], par exemple, envisage des attaques pouvant profiter de la compromission des objets connectés de façon à pouvoir être utilisés dans des attaques de grande envergure ou des botnets.

Un exemple typique est celui des Smart-TVs. Ces téléviseurs aujourd'hui, intègrent un système d'exploitation, divers types de connexions (dont une connexion Ethernet), leur permettant d'offrir de nouveaux services aux utilisateurs. De nouveaux protocoles, tels que HbbTV [1], permettent de combiner l'affichage "classique" des émissions de télévision avec du contenu interactif. En ce qui concerne la sécurité de ces équipements, deux points importants peuvent être envisagés. Tout d'abord, comme pour tout système informatique, le logiciel embarqué dans une Smart-TV peut contenir des vulnérabilités. Et comme les Smart-TVs sont aujourd'hui simultanément connectées à différents types de réseaux (le réseau de diffusion des émissions TV et le réseau Internet, le réseau local de la maison), elles peuvent donc constituer une cible stratégique pour un attaquant puisqu'elles peuvent être utilisées comme passerelle, une fois compromises. Les Smart-TVs peuvent donc représenter une réelle menace pour les réseaux domestiques. Il est donc important d'analyser leur sécurité ainsi que les impacts sur l'ensemble du réseau domestique en cas de compromission.

L'objectif de cet article est de focaliser sur les problèmes de sécurité liées à la connexion des Smart-TVs à différents types de réseaux et de proposer des expérimentations pour analyser ces problèmes. En particulier, nous étudions les compromissions liées à la connexion au réseau numérique de diffusion d'émissions de télévision et de l'utilisation du standard DVB. A notre connaissance, peu de travaux se sont penchés sur ce type de compromission. Cet article présente des expérimentations qui ont été menées sur 4 téléviseurs provenant de 4 différents constructeurs.

L'article est structuré comme suit. La section 2 discute rapidement des différents points d'attaque sur les Smart-TVs et fait état des travaux similaires. La section 3 décrit les différents outils que nous avons utilisés pour nos expérimentations. La section 4 présente les expérimentations que nous avons menées ainsi que leurs résultats. Enfin, la section 5 conclut cet article et présente quelques perspectives.

2 Surface d'attaque d'une Smart-TV

Cette section présente rapidement les différents chemins d'attaques que l'on peut globalement envisager sur une Smart-TV. La figure 1 présente une Smart-TV et ses multiples points de connexion. Les différents chemins d'attaque analysés sont matérialisés par des flèches vertes.

1. Hybrid Broadcast Broadband TV

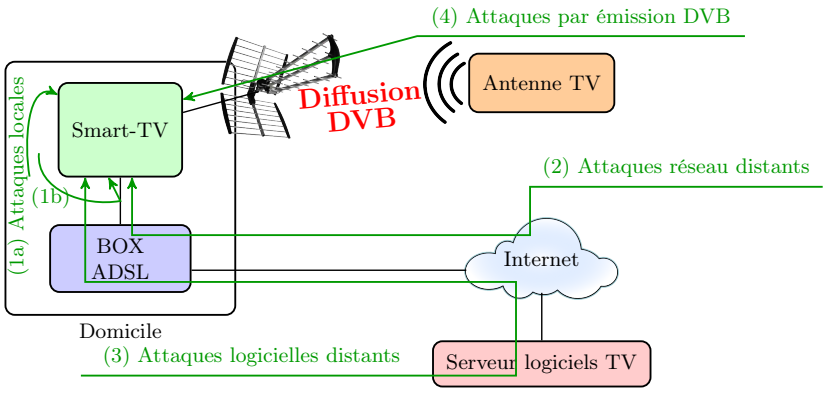

Figure 1. Smart-TV au sein du réseau domestique

2.1 Attaques locales et distantes

Les attaques locales nécessitent un accès physique au téléviseur ($1a$), ou un accès à un des réseaux locaux sur le lequel le téléviseur est connecté ($1b$). Ce type d'attaque est donc exécuté par quelqu'un qui est physiquement proche du téléviseur. Ces attaques sont abordées dans plusieurs articles [15][16][14][11]. De nombreux forums centralisent également des informations sur les méthodes de compromission des téléviseurs ([3] [1]), par exemple, pour modifier ou changer le firmware du téléviseur de façon à activer certaines fonctionnalités cachées.

Les attaques à distance consistent à exploiter, depuis le réseau Internet (2), des vulnérabilités incluses dans le téléviseur connecté au réseau domestique. Ces attaques sont en général très difficiles à réaliser car l'utilisation des techniques de NAT sur le réseau domestique font qu'en général, seule la Box ADSL est accessible depuis le réseau Internet.

Enfin, on peut également envisager les attaques indirectes (3) qui consistent, par exemple, à corrompre le site Web du constructeur du téléviseur ou un site regroupant des applications disponibles pour le téléviseur, de façon à y insérer un firmware ou une application malveillante. Le téléviseur est donc indirectement corrompu lorsqu'il se connecte sur ces sites pour télécharger des mises à jour par exemple, et exécuter ce code malveillant.

2.2 Attaques DVB

Le réseau sur lequel le téléviseur reçoit les émissions de télévision n'est traditionnellement pas considéré comme une source de menaces. Néan-

moins, notre position dans cet article est de bel et bien considérer des menaces pouvant provenir de ce réseau (4). Des faiblesses de la norme DVB ont été présentées récemment dans [12], dans lequel les auteurs abordent notamment les problèmes de vie privée. Des premiers scénarios d'attaque plus élaborés ont été présentés dans [13] mais ils sont essentiellement théoriques et ne présentent pas de résultat précis d'expérimentations. À notre connaissance, il y a donc un manque d'expérimentations concrètes concernant ces chemins d'attaque. Le but de cet article est donc de contribuer à pallier à ce manque en proposant quelques expérimentations concernant la norme DVB.

L'émission hertzienne n'est pas le seul moyen de réception de la télévision en France. En effet, d'autres modes de transmission, tels que l'ADSL ou les liaisons satellites, sont utilisés. Or, d'après l'observatoire de l'équipement audiovisuel des foyers du premier semestre 2014 en France [8], 59% des foyers français reçoivent la télévision par voie hertzienne, dont la moitié ne la reçoit par aucun autre moyen, soit 29% des foyers.

Dans la suite, nous donnons tout d'abord quelques informations sur le standard DVB, puis nous présentons les différents outils que nous avons utilisés pour nos expérimentations. Ces outils nous permettent d'une part d'observer les flux de transport DVB pour en analyser le contenu, et d'autre part de simuler un fournisseur de service utilisant ce standard pour pouvoir mener des attaques.

3 Le standard DVB et les outils d'expérimentations

3.1 La norme DVB

DVB est un ensemble de standards pour la transmission de la télévision numérique [17]. Il s'agit d'une extension des technologies MPEG-TS, qui multiplexe donc différents types de flux audio et vidéo, en y ajoutant des flux de données, contenant des tables de signalisation. Ainsi, chaque flux de transport DVB multiplexe un certain nombre de chaînes TV ainsi que des données. Les chaînes TV sont elles-mêmes décomposées en un certain nombre de flux élémentaires. Les flux de données DVB contiennent, quant à eux, des tables de signalisation. L'une de ces tables, *Application Information Table (AIT)*, contient les paramètres nécessaires au bon fonctionnement du protocole HbbTV (*Hybrid Broadcast Broadband TV*). Ce protocole permet de bénéficier de services interactifs avec les programmes des chaînes TV, tels que des informations sur les programmes diffusés, la possibilité de revoir un film ultérieurement, d'accéder à des guides des programmes, etc. Les différents flux peuvent être acheminés

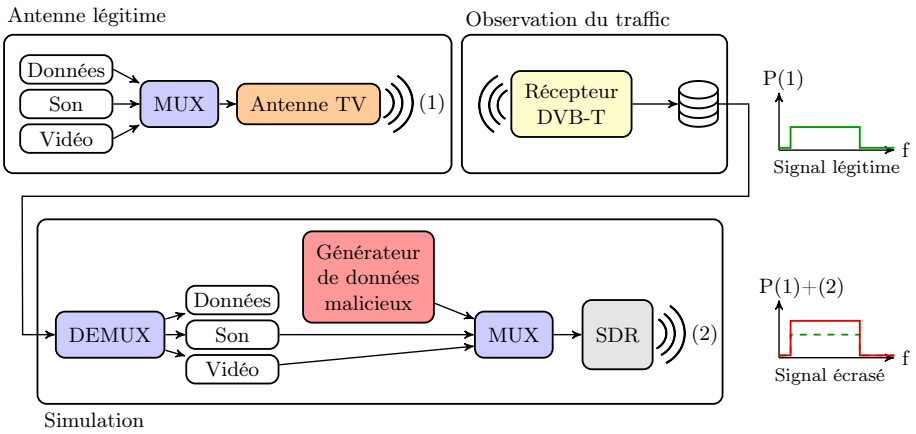

Figure 2. Plateforme d'expérimentations DVB

sur différents supports, tels que le satellite, l'aérien ou le câble. Dans cet article, nous considérons uniquement la transmission aérienne (TNT), également connue sous le nom de transmission terrestre, qui est le support le plus répandu sur la planète [7]. Ce type de transmission est terminé par un démodulateur DVB-T, installé dans le domicile du client, et par un modulateur DVB-T, du côté du fournisseur de service.

3.2 Outils permettant l'observation du trafic

Des outils permettent d'observer tous les flux reçus par un téléviseur réglé sur une certaine fréquence. Comme tous les téléviseurs du marché sont aujourd'hui équipés pour recevoir ces flux, de nombreux outils sont disponibles. Il suffit de se procurer au préalable un démodulateur DVB-T, disponible sur étagère. Des outils tels que DVBSnoop [2] permettent ensuite d'effectuer des analyses sur les différents flux élémentaires multiplexés dans un flux de transport DVB. Nous avons utilisé également l'utilitaire `tzap` [3] de façon à régler notre démodulateur sur une fréquence particulière.

3.3 Outils de simulation

Ces outils sont destinés à simuler des émissions de flux de transport DVB légitimes. Il est nécessaire pour cela de posséder un modulateur

2. http ://dvbsnoop.sourceforge.net/
3. http ://www.linuxtv.org/wiki/index.php/LinuxTV_dvb-apps

DVB-T ainsi qu'un multiplexeur de flux MPEG TS. Des applications open-source telles que ffmpeg [4] et vlc [5], sont capables de générer et moduler des flux MPEG TS. Cependant, ces applications ne peuvent pas être utilisées pour générer un flux de transport DVB valide dans la mesure où elles ne sont pas capables de créer des tables de signalisation DVB correctes. D'autres applications open-source telles que Avalpa OpenCaster [6] en sont capables.

Comme l'émission TV sans licence est interdite dans la plupart des pays, les modulateurs DVB sont généralement non disponibles sur le marché. Pour nos expérimentations, nous avons opté pour deux solutions. La première utilise un matériel [7] spécifique suggéré par OpenCaster et qu'on peut se procurer directement sur Internet. Ce matériel fonctionne avec OpenCaster mais est limité dans ses paramètres de modulation. Par exemple, il ne supporte que les modulations QPSK [8] et QAM16 [9], ce qui réduit grandement la bande passante disponible [10]. Comme la plupart des pays utilisent la modulation QAM64, ce matériel n'est pas capable de simuler entièrement un multiplexeur DVB. Nous avons donc également utilisé une autre plateforme plus chère, mais générique et adaptable. Il s'agit d'un matériel permettant de réaliser de la radio logicielle *Software Defined Radio (SDR)*. Nous avons pour cela opté pour le matériel Ettus N210 et sa carte fille WBX [11]. Grâçe au logiciel GNU-Radio [12], il est possible de paramétrer ce matériel pour n'importe quel type de modulation radio. La popularité du logiciel GNU-Radio nous a permis de trouver aisément un schéma de modulation DVB-T [6] déjà fonctionnel. A l'aide d'une de ces deux solutions matérielles et du logiciel OpenCaster, nous avons pu implémenter un modulateur DVB-T pleinement fonctionnel.

Le type de communication aérienne de DVB-T fait qu'il n'est pas possible de physiquement débrancher l'émetteur légitime et de le remplacer par le nôtre (comme on pourrait le faire facilement avec une connexion filaire). Il est donc nécessaire de faire en sorte que le signal de notre modulateur "écrase" le signal du modulateur DVB-T légitime. Pour cela, il

4. https ://www.ffmpeg.org/
5. http ://www.videolan.org/vlc/
6. http ://www.avalpa.com/the-key-values/15-free-software/33-opencaster
7. Environ 200 euros.
8. Quadrature Phase-Shift Keying.
9. Quadrature Amplitude Modulation
10. Les différents types de modulations permettent des débits plus ou moins importants en fonction du nombre de symboles définis.
11. Environ 2000 euros.
12. http ://gnuradio.org/

suffit d'émettre avec une puissance plus élevée. Bien sûr, dans le cadre de notre expérimentation en laboratoire, t pour des raisons légales, il ne nous était pas possible d'émettre avec une puissance plus élevée que l'émetteur TNT légitime. En revanche, comme notre émetteur est très proche du téléviseur, la puissance d'émission de notre émetteur, telle que perçue par le téléviseur, est suffisamment plus élevée que la puissance d'émission du signal légitime, pour que le téléviseur considère notre signal et ignore le signal légitime. Des seuils sont officiellement définis par L'Union Internationale des Télécommunications [18] de façon à ce qu'un signal plus faible ne puisse interférer sur un signal plus fort. En approchant notre modulateur de notre téléviseur, nous avons atteint ce seuil et donc écrasé le signal légitime (cf. Figure 2).

Soulignons que les expérimentations présentées dans cet article ont été menées à l'intérieur de notre laboratoire uniquement, de telle façon que nous ne perturbions pas d'autres téléviseurs que ceux dédiés à nos expérimentations.

4 Expérimentations et résultats

Nous avons mené des expérimentations sur un panel de 4 téléviseurs connectés de différentes grandes marques. Dans la suite, ils sont anonymement nommés A, B, C et D.

Nous avons mené deux expérimentations, utilisant principalement les outils de simulation DVB. Les outils d'écoute nous ont été utiles pour comprendre le fonctionnement des flux de transport DVB-T, de façon à pouvoir y insérer des données tout en respectant le protocole. Même s'ils ne nous ont pas servi à lancer des attaques, ils ont été très utiles pour la préparation de ces attaques.

La première expérimentation nous a permis tout d'abord de vérifier si les téléviseurs authentifient les émetteurs des flux de transports DVB qu'ils reçoivent. La seconde expérimentation nous a permis de réellement mener une attaque, en fabriquant nos propres flux de transport DVB.

4.1 Modification d'un flux DVB

Cette première expérimentation vise à montrer que les émetteurs des flux DVB ne sont pas authentifiés par les téléviseurs. Nous avons pour cela utilisé nos outils de simulation, pour fabriquer un flux DVB-T en y insérant un flux élémentaire vidéo issu d'une WebCam. Tous les téléviseurs que nous avons testés ignorent le signal légitime dès que notre modulateur

(dont la puissance d'émission perçue par le téléviseur est supérieure à celle de l'émetteur légitime) est activé, et diffusent donc la capture vidéo de notre WebCam, tout en considérant que le flux reçu est bien le flux légitime de la chaîne de télévision en cours. Aucun message d'erreur apparent n'apparaît ni de dysfonctionnement du téléviseur. Nous avons réalisé ce flux DVB-T en capturant une courte séquence d'un flux légitime et en remplaçant un des flux vidéo par notre capture de WebCam.

4.2 HbbTV et le respect de la politique de la même origine

Cette seconde expérimentation est la plus intéressante dans la mesure où elle va profiter du fait que les flux de transport DVB contiennent des flux élémentaires audio, vidéo mais aussi des données, pouvant être interprétées par le téléviseur. Le format de ces données doit donc respecter le standard HbbTV. Nous avons donc, à l'aide des outils présentés précédemment, créé notre propre flux DVB, incluant nos propres données. Cela peut se traduire sous la forme de pages HTML incluses indirectement dans le flux et interprétées par le téléviseur, ou alors sous la forme d'un URL pointant sur des pages HTML situées sur des sites Web accessibles par le téléviseur, dans la mesure où ce dernier est connecté au réseau Internet.

Dans ce cadre, nous avons voulu vérifier le respect de la politique de la même origine (*same-origin security policy*) [19] par le téléviseur, et plus précisément, par le navigateur intégré qui traite les données HbbTV incluses dans les flux DVB. Cette politique doit en principe être implémentée par les navigateurs lorsque ceux-ci exécutent du code (JavaScript par exemple) qu'ils ont téléchargé depuis un site distant. Elle préconise que, si l'exécution du code, provoque l'exécution d'une requête HTTP POST, cette requête ne peut être autorisée directement qu'à destination du même site Internet qui est à l'origine de ce code. Si la requête est à destination d'un site différent (c'est-à-dire dont le nom complet, appelé également *Fully Qualified Domain Name ou FQDN*) est différent de celui du site Web qui a fourni le code exécutable, le navigateur doit au préalable, envoyer une requête "OPTIONS" au site Web avant la requête POST, ou dans le pire des cas, ignorer cette requête.

Pour réaliser cette expérimentation, nous avons donc installé sur Internet un site Web contenant du code JavaScript malveillant. Ce code JavaScript essaie simplement d'exécuter une requête de type HTTP POST sur un site Web différent. Si le browser Web intégré dans le téléviseur, qui exécute ce code JavaScript, implémente correctement la politique de type *same-origin*, il doit nécessairement soit envoyer, avant la requête POST,

une requête “OPTIONS”, telle que représentée dans la figure 3, soit simplement ignorer la requête. Nous avons ensuite multiplexé dans la partie HbbTV du flux DVB, une URL pointant sur ce site Internet.

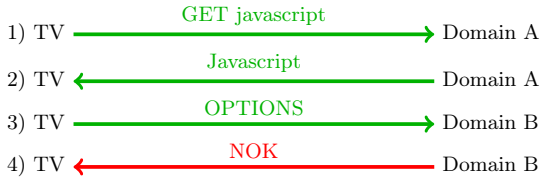

Figure 3. Navigateur web conforme aux politique de la même origine

Nous avons donc testé cette politique de la même origine avec nos 4 téléviseurs Les résultats sont décrits dans le tableau 1.

A	*B*	*C*	*D*
POST	ignore	OPTIONS	OPTIONS

Table 1. Smart-TV et la politique same-origin

Nous constatons que les téléviseurs ont des comportements différents concernant le respect de la politique de la même origine. Les téléviseurs C et D respectent cette politique en envoyant la requête “OPTIONS”, B a une attitude différente en ignorant simplement la requête. En revanche, la téléviseur A exécute directement la requête “POST” et ne respecte donc pas la politique de la même origine.

Il est également possible d’inclure directement le code JavaScript dans une page HTML qui est multiplexé dans le flux DVB. Ce cas est plus complexe, car le browser du téléviseur qui reçoit cette page ne le reçoit pas d’un site Web puisqu’elle provient du flux DVB. Dans ce cas, comment définir l’origine de cette page pour ensuite appliquer la politique de la même origine ? Les auteurs de [13] discutent de ce problème et étudient la possibilité de définir cette origine dans la table AIT, multiplexée dans le flux DVB. A priori, la norme DVB stipule que dans ce cas précis, l’origine est non définie et qu’un paramètre spécifique, *simple_ application_ boundary_ descriptor* [9, S6.3] peut être positionnée par l’émetteur DVB. Cette variable fait office d’origine. Nous avons donc testé cette politique de la même origine avec nos 4 téléviseurs en définissant ce paramètre et en insérant direc-

tement une page HTML contenant du code JavaScript dans les données HbbTV d'un flux de transport DVB. Nous l'avons positionné avec le nom complet FQDN du serveur Web sur lequel nous voulons exécuter la requête POST. Nos expériences ont montré que, le positionnement du paramètre `simple_application_boundary_descriptor` n'a pas d'influence sur le comportement du téléviseur, tout simplement parce-que celui-ci l'ignore. Tous les téléviseurs repositionnent eux-mêmes l'origine de la page Web à une valeur propre au téléviseur, telle que `dvb://1.1.1.b`, lorsque cette page est reçue dans un flux DVB. Nous avons constaté également, dans ce cas, que le comportement des 4 téléviseurs, concernant le respect de la politique de la même origine, est identique au cas précédent. Le téléviseur A ne l'implémente pas correctement.

4.3 Exploitation de la politique de la même origine

Nous avons donc exploité la vulnérabilité du téléviseur A en développant un code JavaScript conçu pour interagir avec la Box ADSL sur laquelle une Smart-TV est en principe connectée au domicile. L'objectif de cette attaque est d'autoriser sur la Box ADSL des connexions sur certains services du téléviseur depuis le réseau Internet. L'utilisation des adresses privées et du NAT dans les réseaux domestiques situés "derrière" une box ADSL, font qu'aujourd'hui, il est impossible d'initier des connexions, depuis Internet, sur une Smart-TV. Si nous arrivons à faire en sorte que ces connexions soient autorisées, nous exposons les Smart-TVs à des attaques provenant de n'importe quel attaquant situé sur le réseau Internet. C'est donc l'objectif de notre attaque. Nous avons développé un petit code JavaScript, installé sur un serveur Web sur le réseau Internet, qui se connecte sur la box ADSL du domicile et demande, via des requête UPNP, l'activation de redirection de port vers le téléviseur. Nous avons ensuite inséré dans les données HbbTV d'un flux de transport DVB, l'URL de ce site Web. Le téléviseur A, a parfaitement exécuté le code JavaScript et exécuté la requête UPNP vers la box ADSL. La majorité des Box ADSL françaises sont aujourd'hui livrées avec le service UPNP activé, ce qui nous a permis de réaliser cette attaque avec succès sur le téléviseur A. Le principe de cette attaque est décrit dans la figure 4.

Le téléviseur A possède un service TCP sur un port particulier qui correspond à une télécommande virtuelle. Il est ainsi possible de se connecter sur ce port pour changer de chaîne, monter le son et exécuter d'autres fonctions qui sont habituellement exécutés grâce à la télécommande du téléviseur. Ce service n'est bien sûr en principe accessible que sur le réseau interne du domicile. Grâce à l'exécution du code JavaScript par notre

navigateur et l'envoi d'une requête "POST" au service UPNP de la Box ADSL, ce service devient donc accessible depuis Internet. Nous avons pu donc réaliser avec succès cette expérimentation. Cette attaque signifie qu'il devient possible pour n'importe quel utilisateur situé sur le réseau Internet d'interagir à distance avec ce type de téléviseur pour monter le son, ou changer de chaîne.

Bien sûr, on peut imaginer des attaques beaucoup plus sérieuses. Les Smart-TVs incluent aujourd'hui un certain nombre de services TCP actifs susceptibles de contenir des vulnérabilités, comme tout service réseau d'un système informatique standard. Diverses vulnérabilités ont d'ailleurs déjà été identifiées et exploitées avec succès dans [4][5]. L'ouverture de ces services à tout utilisateur d'Internet peut permettre à tout attaquant sur ce réseau d'exploiter ces vulnérabilités, qui peuvent mener à la prise de contrôle du téléviseur lui-même. L'intérêt principal de cette preuve de concept est de montrer l'ouverture d'un nouveau chemin d'attaque sur les téléviseurs connectés, ce chemin combinant l'utilisation des flux de transports DVB-T et utilisant une vulnérabilité des navigateurs intégrés dans le téléviseur.

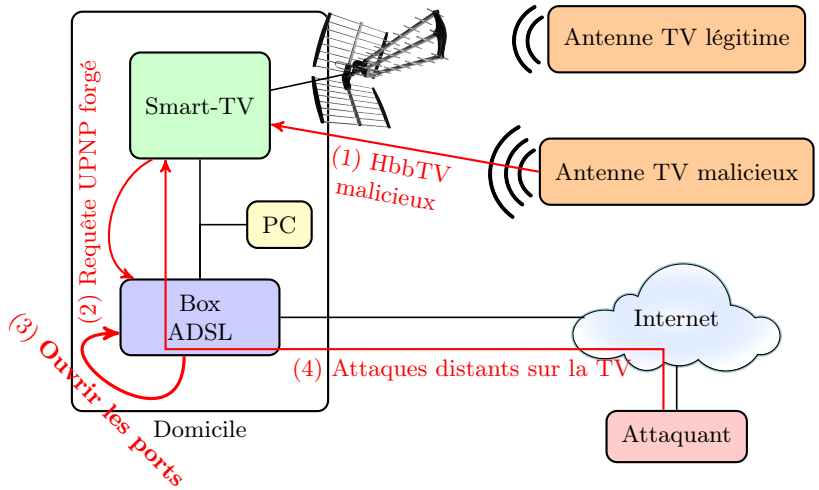

Figure 4. Attaque combinée

5 Conclusion

Dans cet article, nous avons présenté un chemin d'attaque original concernant les Smart-TVs. Ce chemin combine l'introduction de données malveillantes dans un flux de transport DVB et l'exploitation d'une vulnérabilité du logiciel intégré dans le téléviseur qui traite ces flux (logiciel qui n'implémente pas correctement la politique de la même origine). Ce chemin nous a permis d'ouvrir un accès depuis le réseau Internet à potentiellement tous les services fournis par le téléviseur, et par la-même d'exposer les services vulnérables aux attaquants situés sur ce réseau.

Ce nouveau chemin d'attaque montre qu'il est important de s'intéresser à la sécurité des objets connectés dans notre domicile aujourd'hui. Les études de sécurité sur ce type d'objets ne sont pas encore très nombreuses mais de multiples vulnérabilités ont déjà été découvertes. Certes, le chemin d'attaque que nous présentons nécessite l'utilisation d'un modulateur DVB-T et par conséquent, on imagine mal une attaque sérieuse menée par des attaquants isolés. Cependant, elle est tout à fait intéressante pour une organisation ayant des moyens et de réelles ambitions. Par nature, les flux DVB sont des broadcasts, qui atteignent donc simultanément tous les téléviseurs qui sont à portée du signal. Une attaque de grande ampleur est donc possible. Par ailleurs, les contre-mesures existent puisqu'elles consistent d'une part à patcher les navigateurs intégrés dans les Smart-TVs de façon à ce qu'ils implémentent correctement la politique de la même origine (ce qui semble a priori facile à mettre en œuvre) et d'autre part à authentifier les émetteurs de flux de transport DVB (ce qui semble a priori plus compliqué en terme technique et en terme de déploiement).

Comme perspective à court terme de ces travaux, nous envisageons d'étudier plus précisément comment un attaquant ayant pu prendre le contrôle d'un téléviseur par notre chemin d'attaque peut ensuite rebondir pour prendre le contrôle d'autres objets connectés. Nous souhaitons donc analyser comment les attaques peuvent se propager dans le domicile. De façon plus générale, nous comptons généraliser ce type d'analyses de vulnérabilités sur diverses objets connectés, en ayant toujours à l'idée de tirer profit des multiples réseaux sur lesquels ces objets sont simultanément connectés.

Références

1. Openlgtv. `http://openlgtv.org.ru/wiki/index.php/Wiki\_index`.

2. Défense et sécurité nationale. pages 44–45, Paris, France `http://www.elysee.fr/assets/pdf/Livre-Blanc.pdf`, 2013. Direction de l'information légale et administrive.
3. E. U. Altinyurt. Samygo. `http://www.samygo.tv`. SamyGO.
4. F. Basse. Sécurité des ordivisions. 2014.
5. F. Basse. Télévisions connectées : Des objets branchés sécurité ? In *MISC*, September / October 2014.
6. Bogdan. Dvb-t implementation in gnuradio – part 2. `http://yo3iiu.ro/blog/?p=1220`. YO3IIU.
7. European Comission. Special eurobarometer 396 - e-communications household survey. `http://ec.europa.eu/digital-agenda/en/news/special-eurobarometer-396-e-communications-household-survey`, 2013.
8. Conseil Supérieur de l'Audiovisuel. L'équipement audiovisuel des foyers au premier semestre 2014. 2014.
9. European Broadcasting Union. Etsi ts 102 796 v1.2.1. In *Hybrid Broadcast Broadband TV*, November 2012.
10. Nick Feamster. Outsourcing home network security. In *Proceedings of the 2010 ACM SIGCOMM Workshop on Home Networks*, HomeNets '10, pages 37–42, New York, NY, USA, 2010. ACM.
11. M. Ghiglieri and E. Tews. A privacy protection system for hbbtv in smart tvs. In *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, pages 357–362, Jan 2014.
12. MArtin Herfurt. Hbbtv security. 2013.
13. Yossef Oren and Angelos D. Keromytis. From the aether to the ethernet—attacking the internet using broadcast digital television. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 353–368, San Diego, CA, August 2014. USENIX Association.
14. Proofpoint. Samygo. `http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-proof-of-a-Iot-driven-attack.php`. Proofpoint.
15. N. Ruff. Sécurité de l'adsl en france. In *proc. of Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, Rennes, France, June 1st 2006.
16. Nikos Sidiropoulos and Periklis Stefopoulos. Smart tv hacking. In *Research project 1*, Amsterdam, Netherlands, January 2013.
17. J.H. Stott. The dvb terrestrial (dvb-t) specification and its implementation in a practical modem. In *Broadcasting Convention, International (Conf. Publ. No. 428)*, pages 255–260, Sep 1996.
18. International Telecommunication Union. Itu r-rec-bt.1368-11 year=2014. In *Planning criteria, including protection ratios, for digital terrestrial television services in the VHF/UHF bands*.
19. Michal Zalewski. Browser security handbook, part 2. 2008.