Sécurité des équipements grand public connectés à Internet : évaluation des liens de communication

Yann Bachy

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ FÉDÉRALE TOULOUSE MIDI-PYRÉNÉES

Délivré par :

l'Institut National des Sciences Appliquées de Toulouse (INSA de Toulouse)

Présentée et soutenue le *09/07/2015* **par :**

YANN BACHY

Sécurité des équipements grand public connectés à Internet : évaluation des liens de communication

---

JURY

OLIVIER FESTOR	TELECOM Nancy	Rapporteur
JEAN-LOUIS LANET	INRIA (RBA)	Rapporteur
AURÉLIEN FRANCILLON	EURECOM	Examinateur
MOHAMED KAÂNICHE	LAAS-CNRS	Examinateur
OLIVIER LEVILLAIN	ANSSI	Examinateur
JEAN-CHRISTOPHE COURRÈGE	Thales TCS	Directeur de thèse
VINCENT NICOMETTE	INSA Toulouse - LAAS-CNRS	Directeur de thèse
ERIC ALATA	INSA Toulouse - LAAS-CNRS	Directeur de thèse

École doctorale et spécialité :

MITT : Domaine STIC : Réseaux, Télécoms, Systèmes et Architecture

Unité de Recherche :

Laboratoire d'analyse et d'architecture des systèmes

Directeur(s) de Thèse :

Vincent Nicomette, *Eric Alata* et *Jean-Christophe Courrège*

Rapporteurs :

Jean-Louis Lanet et *Olivier Festor*

Remerciements

J'ai réalisé ma thèse au sein du Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) du Centre National de la Recherche Scientifique (CNRS). Je remercie Jean-Arlat, qui a assuré la direction du laboratoire depuis mon arrivée.

Je remercie également Karama Kanoun et Mohamed Kaâniche, qui ont été les responsables successifs de l'équipe Tolérance aux fautes et Sûreté de Fonctionnement informatique (TSF), dont j'ai fait partie durant mes travaux de thèse.

Je remercie naturellement Thales Communications & Security d'avoir financé mes travaux et de m'avoir intégré dans leurs activités durant ces trois années. Je pense particulièrement à mes chefs Remy Daudigny, Nathalie Feyt, Jean-Christophe Courrège et Pierre Forget qui m'ont toujours soutenu. Je souhaite également remercier tous mes collègues chez Thales. Je pense notamment à : Jean-Yves, Vincent, David, Gilles, Thomas, Romain et Oriane.

De manière générale, cette thèse bien sûr, mais, tout d'abord, la recherche en sécurité informatique au LAAS n'existerait pas sans Yves Deswarte. C'est pourquoi je lui exprime ma grande reconnaissance. Sa disparition, le 27 janvier 2014, nous a laissé à tous un grand vide.

En ce qui concerne ma thèse, je dois énormément à mes encadrants et principalement à mon directeur de thèse, Vincent Nicomette, pour sa rigueur mais surtout pour sa constante bonne humeur. Je dois sans doute également beaucoup à sa femme, Cathy, pour avoir laissé à Vincent le temps de relire toute ma prose.

J'adresse également mes sincères remerciements aux membres du jury qui ont accepté de juger mon travail. Je leur suis très reconnaissant pour l'intérêt qu'ils ont porté à mes travaux :

— Olivier Festor, Professeur des Universités, Télécom Nancy
— Jean-Louis Lanet, Professeur des Universités, Inria (RBA)
— Aurélien Francillon, Assistant professeur, Eurecom
— Mohamed Kaâniche, Directeur de recherche, LAAS-CNRS
— Olivier Levillain, Ingénieur en chef des mines, ANSSI
— Jean-Christophe Courrège, Ingénieur, Thales TCS
— Vincent Nicomette, Professeur des Universités, INSA de Toulouse
— Eric Alata, Maître de conférences, INSA de Toulouse

Je remercie bien évidemment tous les doctorants, docteurs, post-doctorants, stagiaires, mais également les permanents de l'équipe TSF que j'ai pu rencontrer. Je pense à Ivan et Joris, qui ont partagé mon bureau et supporté mes téléviseurs. Je pense également à Pierre, Camille et Kalou qui, au fil des années, sont devenus plus que de simples collègues mais de réels amis. Je ne vais pas tous vous citer,

je risquerais d'en oublier. Le plus important n'est pas de retrouver votre nom ici, mais le contact que nous garderons dans l'avenir.

Je pense également à mes amis qui m'ont soutenu et supporté : Amine, McFly, David, Anaïs, Claire, Laureline, Thibaut, Micha, Antoine et Gem'. Je dois également beaucoup à mes parents et à ma famille, sans qui je ne serais pas là où j'en suis aujourd'hui. Un merci particulier à mon père, qui a assumé jusqu'au bout son rôle de professeur de français langue étrangère dans la phase de correction du manuscrit.

Enfin, et pas des moindres, je remercie ma femme, Julie, d'être à mes côtés chaque jour et de m'avoir encouragé jusqu'au bout.

À tous un grand merci.

Table des matières

Introduction

Ce manuscrit de thèse rapporte des travaux menés au Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) du CNRS à Toulouse, dans l'équipe Tolérance aux fautes et Sûreté de Fonctionnement informatique (TSF). Cette thèse a été effectuée dans le cadre d'un partenariat CIFRE avec Thales Communications & Security basé à Toulouse, et se focalise sur la sécurité de leurs équipements grand public connectés à Internet et plus particulièrement à l'évaluation de la sécurité des liens de communication. Dans un premier temps, nous abordons le contexte scientifique dans lequel se situe cette thèse. Puis, dans un deuxième temps, nous présentons la problématique à laquelle cette thèse s'intéresse. Ensuite, dans un troisième temps, nous présentons les objectifs de ce travail de recherche. Enfin, nous présentons le plan de ce manuscrit.

Contexte scientifique

Depuis des décennies, l'équipement technologique de nos domiciles ne cesse d'évoluer et de prendre part activement à notre vie quotidienne. A ce titre, l'utilisation de l'informatique à domicile s'est généralisée dans les années 80. D'abord un outil de travail, elle est également rapidement devenue un outil de loisir. Il en va de même pour le réseau Internet, interconnectant nos domiciles depuis les années 90. Si l'utilisation du réseau Internet au domicile était à l'origine essentiellement consacrée au travail, elle est désormais indispensable pour bon nombre de foyers dans de multiples domaines : achats en ligne, réservations de vacances, gestion des comptes bancaires et beaucoup d'autres tâches administratives, etc. Depuis quelques années, la connexion au réseau Internet a pris une dimension supplémentaire et propose de nouveaux services, avec l'apparition des offres Internet dites "triple-play". Cette dénomination fait référence aux trois services habituellement inclus dans ces offres : 1) l'accès au réseau Internet à proprement parler, 2) la ligne téléphonique et 3) le bouquet de chaînes TV.

L'évolution constante des technologies permet également l'ajout de nouvelles fonctionnalités sur les équipements informatiques existants. Ces avancées technologiques peuvent concerner des équipements sans nécessairement les connecter au réseau Internet, mais elles tendent de plus en plus à profiter de cette connexion. Ainsi, depuis quelques années, la tendance au "tout connecté" est réellement en marche. De plus en plus d'équipements grand public sont aujourd'hui reliés d'une manière ou d'une autre au réseau Internet. Cette connexion leur permet de fournir encore plus de nouveaux services, souvent dans un but d'améliorer l'interactivité avec l'utilisateur. Afin de distinguer cette nouvelle génération d'équipements, il est souvent fait usage du préfixe "Smart", permettant de faire allusion à une certaine intelligence dans cette nouvelle génération d'équipements.

Problématique

Afin de d'intégrer ces nouvelles fonctionnalités, la majorité de ces équipements utilisent des technologies proches d'un ordinateur classique et sont de ce fait équipés de processeurs et d'un système d'exploitation. Ces technologies sont souvent génériques, et permettent en réalité d'exécuter bien plus de tâches que nécessaire. Dès lors, des préoccupations de sécurité, déjà largement intégrées par notre société en ce qui concerne les ordinateurs personnels, deviennent également légitimes pour ces équipements de nouvelle génération. De plus en plus de faits divers rapportant des problèmes de sécurité sur différents équipements connectés, ou des fuites d'informations concernant la vie privée, sont aujourd'hui rapportés dans les médias. Par ailleurs, les industriels et les chercheurs s'intéressent de plus en plus à ces problèmes de sécurité.

Contrairement aux ordinateurs personnels, il n'est généralement pas prévu, par le constructeur de ces équipements, d'offrir à l'utilisateur final la possibilité de modifier ou de remplacer le système d'exploitation qui y est intégré. En effet, quand bien même la majorité des ordinateurs personnels vendus ont un système d'exploitation pré-installé, il est prévu de laisser libre choix à l'utilisateur d'en changer. Il en va de même pour les mises à jour et toute autre tâche de maintenance. Pour les équipements connectés, en revanche, ces opérations sont effectuées selon le bon vouloir du constructeur. L'utilisateur devient en quelque sorte prisonnier du fabricant, premièrement car il ne peut assurer lui-même, ni la sécurité, ni la maintenance de l'équipement qu'il possède, et deuxièmement car il est très difficile de s'assurer de la bienveillance du constructeur, qui pourrait aller jusqu'à inclure du code spécifique à l'intérieur du système d'exploitation, afin, par exemple, d'extraire des données privées concernant l'utilisateur.

Ces équipements sont connectés au réseau local du domicile au même titre qu'un ordinateur personnel, afin de bénéficier de la connexion à Internet. Ceci suppose que :

— Des informations privées contenues dans ces équipements peuvent être renvoyées au fabricant. Par exemple, dans le cas des Smart-TVs, on peut imaginer une divulgation du nom de la chaîne de TV que le téléspectateur est en train de regarder.

— Ces équipements sont vulnérables au même titre qu'un ordinateur personnel relié à ce réseau. Par exemple, on peut imaginer un maliciel, installé sur un équipement, qui est un relais de messagerie pour envoyer des spams.

De plus, certains équipements grand public utilisent déjà un réseau de données, autre qu'Internet, afin d'accéder à du contenu mis à disposition par un fournisseur de services. De ce fait, lorsque ces équipements sont connectés au réseau local pour bénéficier de la connexion à Internet, ceci nous permet de supposer qu'ils peuvent devenir des passerelles entre deux réseaux hétérogènes. Par exemple, on peut imaginer qu'un réseau d'accès unidirectionnel, fournisseur de services et habituellement considéré comme sûr, puisse véhiculer du code malveillant, qui pourrait ensuite se propager sur le réseau Internet ou même sur les autres équipements connectés du

domicile.

Ceci nous semble constituer un réel enjeu aujourd'hui dans la mesure où beaucoup d'équipements connectés disposent de multiples interfaces de communication et peuvent donc constituer un vecteur intéressant de propagation de maliciels. Par exemple, les Smart-TVs ont une connexion avec le fournisseur de contenus télévisuels et une connexion Internet ; un système d'alarme est connecté avec ses capteurs et est connecté au réseau Internet.

Il nous semble donc fondé de mettre en cause la sécurité de cette nouvelle génération d'équipements grand public connectés à Internet et de vouloir analyser en particulier la sécurité de ses liens de communication. Ce manuscrit tente d'apporter des réponses à ces préoccupations.

Objectifs

Cette thèse répond à la problématique établie en proposant, dans un premier temps, une méthode générique d'analyse de la sécurité des équipements grand public connectés à Internet. Dans un second temps, nous appliquons cette méthode à deux cas d'étude. Dans ces deux cas d'étude, nous étudions la sécurité de deux équipements grand public connectés à Internet : premièrement, l'Unité d'Accès Intégré, plus communément connue sous l'appellation de "Box Internet", et secondement, les téléviseurs connectés également connus sous le nom de "Smart-TV". Dans le cadre de ces deux cas d'étude, conformément aux objectifs que nous avons annoncés, nous mettons un accent particulier sur l'analyse de la sécurité des réseaux d'accès de ces équipements, qui constituent, selon nous, des chemins d'attaque intéressants et encore peu analysés.

Plan

Le premier chapitre de cette thèse est consacré à la présentation du contexte scientifique et nous y présentons les différents termes techniques utilisés. Ce chapitre tente de donner une définition d'un "objet connecté" en le différenciant de l'objet communicant. Il se termine par la présentation des travaux connexes en établissant une classification des attaques sur les équipements connectés à Internet.

Le deuxième chapitre est consacré à la méthode d'analyse des équipements grand public connectés à Internet que nous mettons en avant dans ce manuscrit. Cette méthode est constituée d'une phase d'analyse des risques suivie d'une phase d'expérimentations. Dans un premier temps, sont donc présentées les différentes méthodes d'analyse des risques ainsi que leur contexte. A l'issue de la phase d'analyse des risques, nous menons une phase d'expérimentations. Cette seconde phase permet de montrer de manière concrète la faisabilité des scénarios d'attaque menant aux risques identifiés grâce à l'analyse des risques. Dans le cadre de ces travaux, nous nous intéressons particulièrement aux risques portant sur les liens de communication. C'est pourquoi nous proposons une méthode d'expérimentation en trois

étapes : observation, simulation et conduite d'attaque.

Le troisième chapitre est consacré au premier cas d'étude de cette thèse, l'analyse de la sécurité des Unités d'Accès Intégrées. Conformément à la méthode présentée dans le chapitre précédent, nous commençons par une analyse des risques générale des UAI. Dans un second temps, nous présentons une étude comparative des différentes UAI, permettant de mettre en avant des faiblesses dans la conception et l'implémentation de certaines d'entre elles. Puis, nous présentons une analyse de ces faiblesses menant à une exploitation concrète. Nous terminons ce chapitre par une discussion concernant les compétences nécessaires pour réaliser les attaques décrites, et ainsi la vraisemblance d'occurrence de ces scénarios.

Le quatrième chapitre est consacré au second cas d'étude de cette thèse, l'analyse de la sécurité des téléviseurs connectés. Tout comme pour le premier cas d'étude, celui-ci commence par une analyse des risques généralisée des téléviseurs connectés. Ensuite, nous abordons différents aspects de ces téléviseurs connectés. Dans un premier temps, nous étudions les spécificités du canal TV hertzien. Dans un second temps, nous analysons les problèmes de sécurité liés au protocole HbbTV permettant de rendre la télévision interactive. Puis, suite aux failles de sécurité dans les procédures de mise à jour, découvertes lors de l'étude des UAI, nous vérifions la procédure de mise à jour pour les téléviseurs. Enfin, nous terminons par une étude concernant le respect de la vie privée.

Le cinquième chapitre est consacré aux contre-mesures face aux problèmes identifiés au travers de ces deux cas d'étude. Dans la mesure où les vulnérabilités identifiées dans nos travaux concernent des interfaces et des protocoles de communication, nous revenons tout d'abord sur les principes du modèle OSI et les piles de protocoles. Ensuite, nous revenons plus en détail sur les deux cas d'études de cette thèse et en particulier sur les protocoles pour lesquels nous avons mené nos études de vulnérabilités et proposons, pour chacun d'entre eux, des contre-mesures spécifiques pour chaque couche de la pile de protocole, en essayant de discuter les différents paramètres qui peuvent entrer en jeu dans l'application ou non de ces mécanismes de sécurité : l'efficacité, bien sûr, mais aussi le coût de déploiement, les contraintes que ce déploiement peut imposer, etc.

Enfin, la conclusion générale de ce manuscrit présente un bilan de notre travail de recherche, en dégage les principales contributions et propose quelques perspectives qui nous semblent intéressantes.

Chapitre 1

Contexte scientifique & état de l'art

Sommaire

Ce chapitre présente le contexte scientifique de cette thèse. Dans un premier temps, nous définissons un certain nombre de termes employés dans le contexte de cette thèse. Dans un second temps, nous caractérisons les objets grand public connectés à Internet tels que nous les considérons dans le cadre de cette thèse. Nous présentons ensuite les travaux connexes en établissant notamment une classification des attaques existantes. Enfin, nous présentons les contributions de cette thèse.

1.1 Définitions

Dans un premier temps, nous présentons quelques définitions relatives au domaine de la sûreté de fonctionnement. Ensuite, nous abordons quelques termes parmi les nombreux qui viennent enrichir le vocabulaire du domaine des objets connectés. Ces termes sont, pour la plupart, issus de nouvelles avancées technologiques et ils permettent généralement de regrouper des familles technologiques. Il n'existe, à notre connaissance, pas toujours de définition "officielle" de ces termes, et c'est la raison pour laquelle nous souhaitons en proposer une dans ce manuscrit.

1.1.1 La sûreté de fonctionnement

La sûreté de fonctionnement [10] d'un système informatique est *la propriété qui permet à ses utilisateurs de placer une confiance justifiée dans le service qu'il leur délivre*. Le service délivré par un système est son comportement tel qu'il est perçu par son, ou ses utilisateurs, l'utilisateur étant un autre système, humain ou physique qui interagit avec le système considéré. La sûreté de fonctionnement peut être représentée par l'arbre représenté dans la Figure 1.1.

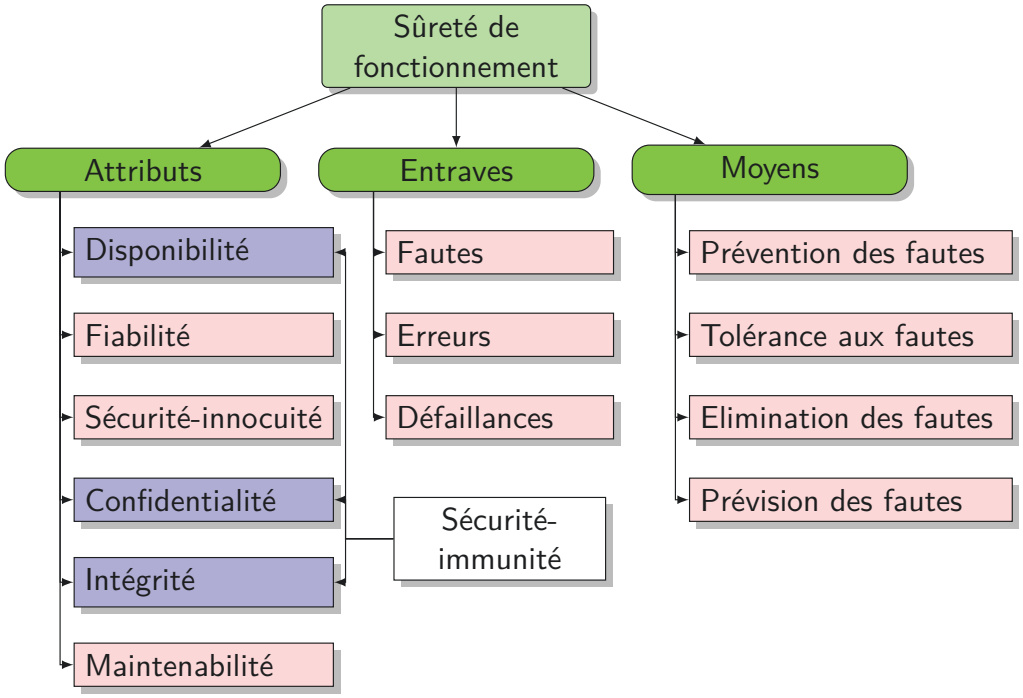


FIGURE 1.1 – La sûreté de fonctionnement

1.1.1.1 Attributs de la sûreté de fonctionnement

Les attributs de la sûreté de fonctionnement permettent a) d'exprimer les propriétés qui sont attendues du système, et b) d'apprécier la qualité du service délivré, tels que le résultat des entraves et des moyens de s'y opposer. Les attributs de la sûreté de fonctionnement sont définis de la manière suivante :

- le fait d'être prêt à l'utilisation conduit à la **disponibilité** ;
- la continuité du service conduit à la **fiabilité** ;
- la non-occurrence de conséquences catastrophiques pour l'environnement conduit à la **sécurité-innocuité** ;
- la non-occurrence de divulgations non-autorisées de l'information conduit à la **confidentialité** ;
- la non-occurrence d'altérations inappropriées de l'information conduit à l'**intégrité** ;

— l'aptitude aux réparations et aux évolutions conduit à la **maintenabilité**.

L'association, à la confidentialité, de l'intégrité et de la disponibilité vis-à-vis des actions autorisées, conduit à la sécurité-confidentialité ou encore la sécurité-immunité. Il existe également d'autres attributs, secondaires, que ceux définis ci-dessus [4]. Un exemple d'un tel attribut secondaire est la robustesse, à savoir, la fiabilité par rapport aux défauts externes, qui caractérise la réaction d'un système par rapport à une classe spécifique de fautes. Nous discutons plus en détail les trois attributs de la sécurité-immunité et les attributs secondaires dans la section 1.1.1.4.

Les attributs de la sûreté de fonctionnement ont été définis selon diverses propriétés, sur lesquelles on peut mettre un accent plus ou moins prononcé selon l'application à laquelle est destiné le système informatique considéré :

— la disponibilité est toujours requise, bien qu'à des degrés naturellement variables selon les applications ;
— fiabilité, sécurité-innocuité, confidentialité peuvent être ou ne pas être requises selon les applications.

1.1.1.2 Entraves à la sûreté de fonctionnement

Les entraves à la sûreté de fonctionnement sont les circonstances indésirables — mais non inattendues — causes ou résultats de la non-sûreté de fonctionnement (dont la définition se déduit simplement de celle de la sûreté de fonctionnement : la confiance ne peut plus, ou ne pourra plus, être placée dans le service délivré). Les entraves à la sûreté de fonctionnement sont : fautes, erreurs, défaillances. Les mécanismes de création et de manifestation des fautes, erreurs, défaillances peuvent être résumés comme suit :

1. Une faute est **active** lorsqu'elle produit une erreur. Une faute active est soit une faute interne qui était préalablement **dormante** et qui a été activée par le processus de traitement, soit une faute externe. Une faute interne peut cycler entre ses états dormant et actif. Les fautes physiques ne peuvent affecter directement que des composants matériels, alors que les fautes dues à l'homme peuvent affecter n'importe quel type de composant.
2. Une erreur peut être latente ou détectée ; une erreur est **latente** tant qu'elle n'a pas été reconnue en tant que telle ; une erreur est **détectée** par un algorithme ou un mécanisme de détection. Une erreur peut disparaître sans être détectée. Par propagation, une erreur crée de nouvelles erreurs.
3. Une défaillance survient lorsque, par propagation, elle affecte le service délivré par le système, donc lorsqu'elle "passe à travers" l'interface système-utilisateur(s). La conséquence de la défaillance d'un composant est une faute pour le système qui le contient ou pour le, ou les composants qui interagissent avec lui ; les modes de défaillance d'un composant sont donc des types de fautes pour le système ou pour les composants qui interagissent avec lui.

Ces mécanismes permettent de compléter la "chaîne fondamentale" suivante :

... → défaillance → faute → erreur → défaillance → faute → ...

Les flèches dans cette chaîne expriment la relation de causalité entre fautes, erreurs et défaillances. Elles ne doivent pas être interprétées au sens strict : par propagation, plusieurs erreurs peuvent être créées avant qu'une défaillance ne survienne ; une défaillance étant un événement se produisant à l'interface entre deux systèmes ou composants, une erreur peut conduire à une faute sans que l'on observe de défaillance si l'observation de la défaillance n'a pas lieu d'être effectuée, ou si elle ne présente pas d'intérêt.

1.1.1.3 Les moyens pour la sûreté de fonctionnement

Les moyens pour la sûreté de fonctionnement sont des méthodes et techniques permettant de fournir au système l'aptitude à délivrer un service conforme à l'accomplissement de sa fonction, et de donner confiance dans cette aptitude. Les méthodes pour la sûreté de fonctionnement sont :

- La **prévention de fautes** : comment empêcher l'occurrence ou l'introduction de fautes ;
- La **tolérance aux fautes** : comment fournir un service à même de remplir la fonction du système en dépit des fautes ;
- L'**élimination des fautes** : comment réduire la présence (nombre, sévérité) des fautes ;
- La **prévision des fautes** : comment estimer la présence, la création et les conséquences des fautes.

La prévention de fautes [4] est obtenue par la mise en œuvre de techniques d'ingénierie rigoureuses pendant les phases de conception et de développement du matériel et des logiciels. Ces techniques incluent la programmation structurée, le masquage d'information, la modularisation, etc., pour les logiciels, et les règles rigoureuses de conception pour le matériel. Blindage, durcissement au rayonnement, etc., ont pour but d'empêcher des défauts physiques opérationnels, tandis que la formation et les procédures rigoureuses pour l'entretien, ont pour but d'éviter les problèmes d'interaction. Les pare-feux et les défenses similaires sont destinés à éviter les problèmes malveillants.

La tolérance aux fautes [14] est mise en œuvre par le traitement des erreurs et par le traitement des fautes [8]. Le traitement d'erreur est destiné à éliminer les erreurs, si possible avant qu'une défaillance ne survienne. Le traitement de faute est destiné à éviter qu'une, ou des fautes ne soient activées à nouveau.

L'élimination des fautes est constituée de trois étapes : vérification, diagnostic, correction. La **vérification** consiste à déterminer si le système satisfait des propriétés, appelées conditions de vérification [57] ; si ce n'est pas le cas, les deux autres étapes doivent être entreprises : diagnostiquer la ou les fautes qui ont empêché les conditions de vérification d'être remplies, puis apporter les corrections nécessaires. Après correction, le processus doit être recommencé afin de s'assurer que l'élimination de faute n'a pas eu de conséquences indésirables ; les vérifications ainsi effectuées sont généralement qualifiées de **non-régression**.

La prévision des fautes est conduite en effectuant des évaluations du comportement du système par rapport à l'occurrence des fautes et à leur activation. En adoptant une vue structurelle d'un système, l'évaluation consiste à examiner et analyser les défaillances des composants et leurs conséquences sur la sûreté de fonctionnement du système.

1.1.1.4 La sécurité-immunité

Dans cette thèse nous nous intéressons essentiellement à la sécurité-immunité, nommée simplement sécurité par la suite s'il n'y a pas d'ambiguïté avec la sécurité-innocuité. La sécurité-immunité peut être définie par les trois attributs (cf. Figure 1.1) [41] : disponibilité, intégrité et confidentialité. Il existe également des attributs secondaires et des entraves propres à la sécurité-immunité que nous définissons dans cette section.

Disponibilité

La disponibilité est la propriété d'une information d'être accessible lorsqu'un utilisateur autorisé en a besoin. Cela signifie que le système informatique doit :

— fournir l'accès à l'information pour que les utilisateurs autorisés puissent la lire ou la modifier ;
— faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information.

La disponibilité implique l'intégrité, puisqu'il ne servirait à rien de rendre accessible une information fausse. La disponibilité implique également des contraintes plus ou moins précises sur le temps de réponse du système. La propriété de disponibilité s'applique aussi au *service* fourni par le système informatique et une atteinte contre la disponibilité est souvent appelée *déni de service*.

Intégrité

L'intégrité est la propriété d'une information de ne pas être altérée. Cela signifie que le système informatique doit :

— empêcher une modification [1] indue de l'information, c'est-à-dire une modification par des utilisateurs non autorisés ou une modification incorrecte par des utilisateurs autorisés ;
— faire en sorte qu'aucun utilisateur ne puisse empêcher la modification légitime de l'information ; par exemple, empêcher la mise à jour périodique d'un compteur de temps serait une atteinte contre l'intégrité.

1. Le terme de modification doit être entendu au sens large, comprenant à la fois la création d'une nouvelle information, la mise à jour d'une information existante et/ou la destruction d'une information.

Confidentialité

La confidentialité est la propriété d'une information de ne pas être révélée à des utilisateurs non autorisés à la connaître. Ceci signifie que le système informatique doit :

— empêcher les utilisateurs de lire une information confidentielle (sauf s'ils y sont autorisés) ;
— empêcher les utilisateurs autorisés à lire une information de la divulguer à d'autres utilisateurs (sauf autorisation) ; ce deuxième point est souvent négligé, car plus difficile à assurer.

Attributs secondaires

La notion d'attributs secondaires est particulièrement pertinente pour la sécurité-immunité, lorsque nous distinguons différents types d'information. Des exemples de tels attributs secondaires sont :

— **Responsabilité** : la disponibilité et l'intégrité de l'identité de la personne qui a réalisé une opération.
— **Authenticité** : c'est la propriété d'être "vrai". Pour un message, l'authenticité est équivalente à l'intégrité à la fois du contenu du message (intégrité des *informations*) et de son origine (*méta-information*), ainsi qu'éventuellement d'autres méta-informations telles que l'instant d'émission ou le niveau de classification (intégrité des *méta-informations*). De la même manière, un document est authentique si son contenu n'as pas été altéré (intégrité des *informations*) et optionnellement si l'auteur déclaré est vraiment l'auteur et non un plagiaire, si la date de publication est correcte, etc. (intégrité des *méta-informations*). De la même manière, un utilisateur prétendu est authentique si l'identité déclarée est bien la bonne identité de cette personne. L'*authentification* est le processus qui donne confiance dans l'authenticité.
— **non-Répudiabilité** : la disponibilité et l'intégrité de l'identité de l'émetteur d'un message (non-répudiabilité de l'origine), ou du destinataire (non-répudiabilité de la réception).

Entraves

La sécurité-immunité définit également ses propres entraves et menaces, à travers les notions de **vulnérabilité, d'attaque et d'intrusion** [4] :

— **Attaque** - Une faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité ; c'est une tentative d'intrusion.
— **Vulnérabilité** - Une faute créée durant le cycle de développement du système, ou durant son fonctionnement, qui peut être exploitée afin de créer une intrusion.

— **Intrusion** - Une faute malveillante interne, mais d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité.

1.1.2 Les équipements grand public connectés à Internet

Après avoir donné les définitions principales du domaine de la sûreté de fonctionnement, et en particulier celles qui concernent la sécurité-immunité, au centre de ce travail de thèse, cette section est consacrée à quelques définitions de termes concernant les équipements grand public connectés à Internet.

1.1.2.1 Web 3.0

L'évolution constante des technologies, que nous avons en partie abordée dans l'introduction, existe également dans le monde du Web. En seulement quelques années, ce qui était initialement un ensemble de pages statiques sont devenues de réelles interfaces dynamiques et participatives. Afin de marquer cette évolution majeure, le terme "Web 2.0" a été introduit dès 2004. D'abord utilisé par tout un chacun sans réelle définition, il a rapidement été nécessaire d'en définir le sens. Plusieurs experts du domaine se sont livrés à l'exercice [52, 9] et ont proposé une définition. Celle qui semble le plus souvent citée est celle de Tim O'Reilly [80], que nous reportons ici littéralement :

Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an "architecture of participation," and going beyond the page metaphor of Web 1.0 to deliver rich user experiences. [79]

Ce que l'on peut retirer de cette définition est que le Web 2.0 tend à définir un Internet plus interactif et participatif, qui met l'individu au cœur du système [78]. L'ensemble des outils permettant de faciliter la collaboration et le partage d'informations sur Internet (les outils collaboratifs tels que les Wikis mais aussi tous les réseaux sociaux informatiques, à l'image de Facebook) font partie de ce Web 2.0. Ce terme et sa définition sont aujourd'hui globalement adoptés. Depuis, toute une nomenclature de versions a vu le jour, accentuant l'idée qu'on puisse définir différentes ères du Web. Sans discuter toutes les versions proposées, nous nous arrêtons sur l'introduction du "Web 3.0" [84]. En effet, du fait de son nom, elle laisse supposer une nouvelle version majeure. Les différentes définitions de ce nouveau terme apportent des aspects intéressants dans le contexte scientifique de cette thèse. Là ou le "Web 2.0" identifie les avancées d'un point de vue utilisation, le "Web 3.0" se focalise sur les évolutions structurelles et architecturales [88]. Ces évolutions se traduisent par des notions de "Web sémantique" et d'"Internet des Objets" [54].

Web sémantique

Le Web sémantique est un terme défini pour la première fois en 2001 [23]. Le Web sémantique y est défini comme une extension du Web actuel. Il s'agit d'une philosophie d'évolution des technologies du Web. Actuellement, les données sur le Web sont transmises de telle sorte que, seul un utilisateur peut les interpréter facilement (ex. : les horaires d'ouverture d'un magasin). Dans un Web sémantique, ces données sont transmises de telle manière qu'un ordinateur puisse les interpréter de manière autonome sans intervention humaine. Il s'agit d'offrir aux systèmes informatiques la même base de connaissances (et son interprétation) que celle qu'obtient un humain en analysant une page Web.

Internet des Objets

L'Internet des Objets, traduction littérale de l'anglais "Internet of Things" (IoT), est une expression apparue au début des années 2000 avec la création du laboratoire de recherche Auto-ID au MIT. À la même époque, des études de marché, notamment sur le commerce mobile [28], annoncent l'intégration d'une certaine intelligence dans des équipements grand public afin qu'ils soient capables de se connecter au contenu et commerce sur Internet. Dans [22], les auteurs proposent de définir l'Internet des Objets comme *"un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant"*. Cette définition met en avant une interconnexion massive de tous les objets qui nous entourent, introduisant ainsi de nouveaux besoins d'identification et de communication. De plus, une notion d'ubiquité est introduite, ce qui donne tout son sens au besoin de données sémantiques, et ainsi le Web sémantique.

Globalement, on peut retenir, que le Web n'est plus uniquement un moyen d'échange homme / machine. Les objets de notre quotidien sont aujourd'hui connectés au Web, capables de communiquer avec nous, mais également capables de communiquer entre eux [29]. Les *objets connectés* et *communicants* (cf. section suivante) deviennent dès lors des acteurs primordiaux de l'Internet de demain.

1.1.2.2 Objets Intelligents

Les objets intelligents jouent un rôle essentiel dans l'Internet de demain. Dans cette section nous distinguons deux catégories d'objets intelligents.

Objets communicants

Un objet communicant est un objet capable d'informer les équipements de son entourage sur son état. L'objet communicant n'effectue, en principe, pas de traitement sur les données qu'il envoie.

Le premier objet communicant au monde est sans doute le distributeur de sodas à l'université de Carnegie Mellon dans le département informatique [96]. L'histoire raconte que la lassitude de se trouver face à une machine vide, ou remplie de sodas encore tièdes, a incité certains chercheurs de cette université à trouver une solution à ce problème. Quatre personnes ont alors installé des micro-capteurs à l'intérieur de la machine qu'ils ont reliés au serveur central de l'université. Ils ont alors développé un logiciel capable de calculer le nombre de sodas à l'intérieur de la machine ainsi que l'heure à laquelle chaque soda est arrivé dans la machine. Grâce à quelques capteurs, une carte électronique et du code informatique, cette machine était désormais capable de communiquer sur son état.

Il existe aujourd'hui une multitude d'exemples d'objets communicants, jusqu'aux brosses à dents [65] ou les fourchettes communicantes [91]. Tous ces objets communicants sont capables d'informer l'utilisateur de l'état qui leur est propre. Ainsi, à l'aide d'une application mobile, les brosses à dents sont capables désormais d'informer l'utilisateur sur la durée et l'efficacité du brossage qu'il est en train de réaliser, alors que les fourchettes sont capables d'aider l'utilisateur à mieux manger. D'autres solutions [73] permettent, grâce à l'ajout de capteurs communicants, nommées "cookies", de transformer n'importe quel objet du quotidien en objet communicant. Ces cookies intègrent des capteurs très précis capables de mesurer la température, l'humidité ou des mouvements très précis. Ainsi, accrochés à un arrosoir par exemple, ces cookies sont capables de déterminer si les plantes ont été arrosées. La précision des capteurs permet de différencier le mouvement d'un arrosage et celui d'un déplacement de l'arrosoir.

Objets connectés

Jusqu'à présent, nous avons uniquement abordé les objets communiquant sur leur état. Le traitement des données ou l'intelligence à proprement parler, se situe dans une application, souvent mobile, ou à l'intérieur d'un autre équipement connecté. Cette deuxième catégorie correspond aux objets connectés qui utilisent une connexion à Internet afin d'enrichir l'étendue de leurs fonctionnalités. Aujourd'hui, de nombreux équipements grand public deviennent connectés, comme par exemple, les téléviseurs ou les réfrigérateurs. Ces équipements remplissent toujours leur fonction d'origine (comme permettre de regarder des émissions télévisuelles ou conserver les aliments au frais) mais la connexion à Internet leur permet de proposer des services supplémentaires. Il est alors possible de regarder des émissions télévisées à la demande et de commander automatiquement ses courses lorsque les aliments à l'intérieur du réfrigérateur sont consommés. Ce dernier exemple est

d'autant plus intéressant lorsque les aliments à l'intérieur du réfrigérateur sont capables de communiquer avec ce dernier, et sont de ce fait eux-mêmes des objets communicants. Dans ce cas précis, on suppose que les aliments sont dotés de capteurs [37, 47], capables de communiquer sur leur état (date d'achat, quantité, date de péremption, etc.). Ainsi, compte tenu de l'étendue et la variété des aliments (objets communicants) pouvant se trouver à l'intérieur d'un réfrigérateur, la sémantique des données, nécessaire à une co-habitation d'objets provenant d'origine et de constructeurs différents, prend ainsi, une nouvelle fois, tout son sens.

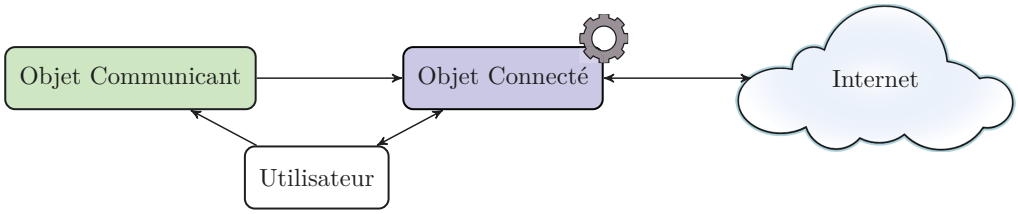


FIGURE 1.2 – Objets intelligents : interactions

On peut donc aisément distinguer deux types d'objets dits "Intelligents". La première catégorie, les objets communicants, peut se résumer à des capteurs ou des objets enrichis de capteurs et d'un moyen de communiquer sur l'état de ce capteur. La deuxième catégorie, les objets connectés, intègre elle-même un certain niveau d'intelligence, capable d'exploiter les informations provenant d'objets communicants. Ces objets possèdent également une connexion à Internet afin d'enrichir l'étendue de leurs fonctionnalités. La Figure 1.2 montre la différence entre les interactions possibles pour ces deux catégories d'objets. Dans la suite de ce chapitre, nous nous intéressons particulièrement aux objets connectés, d'abord en les caractérisant dans la section 1.2, puis en abordant l'aspect sécurité de ces objets dans la section 1.3.

1.2 Caractérisation d'un objet connecté

Cette thèse s'intéresse à la sécurité des équipements grand public connectés à Internet, également connus sous le nom d'"objets connectés". Ainsi, n'importe quel équipement pouvant se trouver dans le domicile d'un particulier et être connecté à Internet, est concerné par notre étude. Un certain nombre d'exemples ont déjà été cités ci-dessus. Cependant, il en existe bien d'autres. Cette section est destinée à caractériser ces objets. Pour cela, dans un premier temps, nous discutons de l'architecture générale de ces équipements. Puis, dans un second temps, nous abordons les entrées / sorties génériques d'un objet connecté ainsi que les systèmes d'exploitation utilisés. Enfin, nous terminerons cette section en abordant l'environnement d'un équipement connecté.

1.2.1 Architecture générale

Un équipement connecté est tout d'abord un équipement réalisant une certaine fonction, comme par exemple un réfrigérateur, un téléviseur ou un téléphone. L'équipement bénéficie d'une connexion à Internet afin d'enrichir sa fonction initiale. La quasi-totalité de ces équipements intègre aujourd'hui des composants semblables à ceux que l'on peut trouver dans un ordinateur personnel. En effet, ils sont dotés de processeurs, de mémoire vive, de stockage de masse et d'interfaces d'entrées/sorties. D'un point de vue logiciel, ces équipements embarquent un système d'exploitation, plus généralement connu sous le nom de "firmware". Cependant, afin d'optimiser les coûts par rapport à un ordinateur, le fabricant intègre généralement "juste ce qu'il faut" afin d'implémenter les fonctionnalités nécessaires. Ceci implique des puissances de calcul réduites, des espaces de stockage limités, des interfaces d'entrées/sorties correspondant aux fonctionnalités de l'équipement ainsi qu'un système d'exploitation limité aux fonctionnalités prévues par le fabricant.

1.2.2 Entrées & Sorties

Les entrées/sorties (E/S) varient d'un système à un autre, en fonction des besoins, des services à fournir ainsi que des avancées technologiques du moment. Il est donc difficile de fournir une liste exhaustive de toutes les E/S pouvant exister parmi tous les objets connectés existants. Cependant, nos travaux nous ont permis d'en lister un certain nombre. Le Tableau 1.1 référence cette liste, divisée en cinq catégories en fonction de leur utilisation. De plus nous avons regroupé les E/S par type (colonne 1), et nous avons défini pour chacune d'entre elles leur périmètre de fonctionnement (colonne 2).

Les cinq catégories d'utilisation que nous avons retenues concernant les E/S sont les suivantes :

- **Homme-Machine** : Interface homme-machine directement intégrée à l'équipement.
- **Périphérique** : Connectivité permettant de relier des équipements périphériques au système.
- **Service distant** : Connectivité permettant de relier le système à un réseau fournisseur de contenu correspondant à l'usage "historique" du système.
- **Internet** : Connectivité permettant de relier le système, éventuellement par le biais du réseau informatique domestique, au réseau Internet.
- **Constructeur** : Connectivité permettant des tests en production ou un service après vente, ces interfaces ne sont pas destinées à l'utilisateur final.

On peut déjà noter que certaines E/S peuvent avoir 2 cas d'utilisation. Par exemple, le Réseau Téléphonique Commuté Public (RTCP) peut à la fois offrir un service téléphonique, comme servir d'accès à Internet en utilisant des technologies xDSL. D'autre part, certains équipements peuvent être reliés à deux réseaux à la fois, l'un servant à fournir un service historique, qui correspond à la principale fonction accomplie par l'équipement, l'autre à accéder à Internet.

Type	Dist	**Entrées / Sorties**	Homme-Machine	Périphérique	Service Distant	Internet	Constructeur
φ^2	1	Ecran	✓				
	1	Touches	✓				
Filaire	1	USB		✓			
	1	eSata		✓			
	1	Fire-Wire		✓			
	1	VGA, HDMI, DVI, Peritel		✓			
	1	LAN (filaire)				✓	
	3	DVB-C			✓	✓	
	3	RTCP			✓	✓	
	3	Fibre				✓	
	3	Secteur			✓[3]	✓	
	1	*Série / JTAG*[4]					✓
Sans-fils	2	IR & RF		✓			
	2	WiFi				✓	
	3	WiMax				✓	
	3	3G, 4G, ...				✓	
	3	GSM			✓		
	3	DVB-S			✓	✓	
	3	DVB-T			✓		

2. Entrées/Sorties **physiques**, directement intégrées à l'équipement.
3. On considère ici l'apport énergétique du réseau électrique comme un service distant.
4. Ces E/S sont généralement dissimulées à l'intérieur de l'équipement.

Tableau 1.1 – Entrées / Sorties

La connectique utilisée par chacune des E/S a un périmètre de fonctionnement défini par la technologie utilisée. Ainsi, par exemple, la portée d'un réseau WiFi est généralement bien inférieure à celle d'un réseau WiMax. De ce fait, nous avons défini trois périmètres de fonctionnement :

1. **Domicile** : le rayon d'action de l'E/S est cantonné à l'intérieur du domicile.
2. **Courte portée** : le rayon d'action de l'E/S est cantonné à un périmètre de quelques mètres du domicile.
3. **Longue portée** : le rayon d'action de l'E/S est au-delà de quelques mètres du domicile.

1.2.3 Système d'exploitation & applications

Les systèmes d'exploitation et applications embarqués dans un équipement connecté, sont généralement connus sous le nom de "firmware". À l'origine, ce terme désignait le microcode CPU se trouvant entre les couches matérielles et logicielles. Cependant, sa définition a rapidement été étendue et définie par l'IEEE [59] de la manière suivante : *The combination of a hardware device and computer instructions and data that reside as read-only software on that device.* Aujourd'hui, ce terme est

utilisé pour désigner le code informatique, c'est-à-dire le système d'exploitation et les applications, embarqués dans un équipement. L'utilisation d'un firmware dans un équipement connecté, offre une plus grande flexibilité au fabricant. En effet, grâce à celui-ci, il peut aisément faire évoluer son produit sans modifications matérielles.

On distingue globalement trois types de firmware. Pour le premier, les firmwares sont spécifiquement développés par le fabricant pour chaque équipement. Ce premier type de firmware équipe généralement des appareils professionnels ou industriels, pour lesquels le fabricant souhaite conserver la maîtrise complète du cycle de développement, comme par exemple dans le cas de systèmes critiques. Pour le deuxième, le fabricant utilise des composants logiciels existants afin de construire son propre firmware. Pour le troisième, le fabricant utilise un firmware générique qu'il personnalise en fonction des besoins du système. Le choix du type de firmware est orienté par une multitude de critères, comme le coût ou l'interopérabilité par exemple. En effet, l'utilisation de composants logiciels gratuits réduit considérablement le coût de développement d'un firmware. De plus, leur utilisation favorise l'interopérabilité entre différents équipements. C'est pourquoi la majorité des équipements grand public intègrent des firmware du deuxième type, et parfois du troisième. Cependant, l'usage de composants logiciels communs peut s'avérer problématique d'un point vue sécurité, si ces composants contiennent des vulnérabilités, qui peuvent ainsi affecter de nombreux équipements [50].

Dans une grande majorité de cas, le fabricant intègre également une solution d'ajout de fonctionnalités (plugins). Ceci offre la possibilité à un tiers de développer des fonctionnalités supplémentaires pour un équipement. L'intérêt pour un développeur tiers, s'il n'est pas directement financier, est corrélé au nombre d'équipements potentiellement ciblés.

1.2.4 Environnement

De manière générale, un équipement grand public s'utilise au domicile de l'utilisateur. Cependant, des terminaux mobiles, comme les Smart-Phones ou tablettes, peuvent, grâce à une batterie, fonctionner en autonomie partout sur la planète. Il est donc possible que plusieurs équipements grand public connectés à Internet cohabitent à l'intérieur du domicile. Certains objets peuvent se révéler plus vulnérables en présence d'un autre objet. Ceci implique qu'il est important de considérer l'environnement d'un équipement, lors d'une analyse de sécurité. De manière générale, nous retenons la traduction d'adresses et l'effet passerelle comme deux facteurs importants liés à un environnement grand public. La Figure 1.3 donne un aperçu global d'un domicile avec des objets connectés.

1.2.4.1 Traduction d'adresse

Sur Internet, chaque équipement (téléphone portable, box, etc.) est en possession d'une adresse IP (*Internet Protocol*) publique et unique. Grâce à cette adresse, tout ce qui est directement connecté à Internet devient accessible depuis n'importe quel

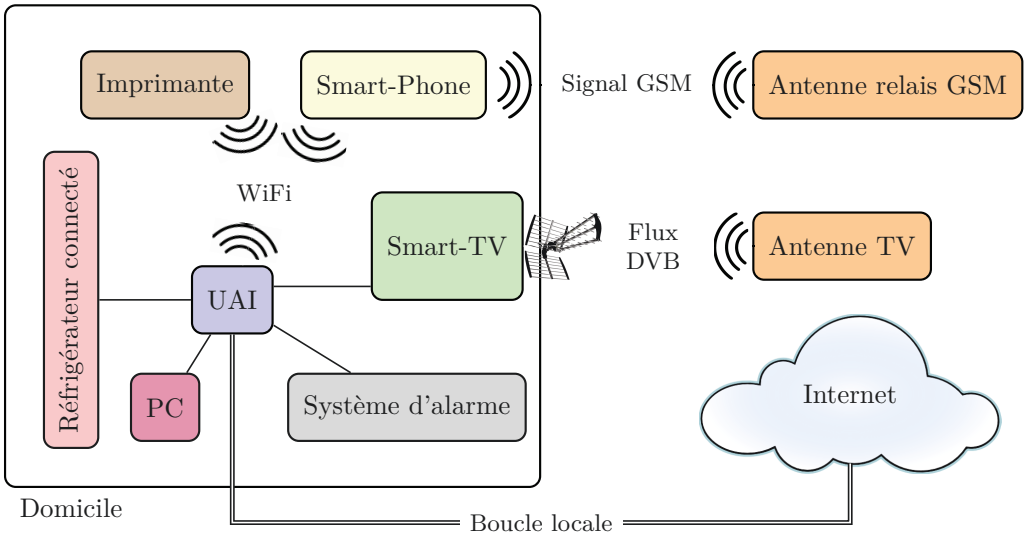


FIGURE 1.3 – Exemple de domicile avec des objets connectés

endroit de l'Internet.

La première version d'IP largement déployée est la version 4. C'est aujourd'hui encore la version la plus utilisée d'IP. Cette version d'IP ne permet que 4 milliards (2^{32}) d'adresses IP. Afin de pallier ce manque d'espace d'adressage, une technique de traduction d'adresses réseaux (NAT) [100] a été introduite. Cette technique est principalement utilisée pour les réseaux domestiques. En effet, pour chaque réseau domestique connecté à Internet en France, seul l'équipement de bordure, l'unité d'accès intégrée (UAI), possède une adresse IP publique. Les autres équipements domestiques, tels que les ordinateurs, téléviseurs connectés, lecteurs multimédia, systèmes d'alarmes, etc., se voient attribuer une adresse IP privée (en général par l'UAI elle-même) qui doit être traduite afin de permettre à l'équipement d'accéder à Internet.

Sur la Figure 1.3, on aperçoit que seul l'UAI est en communication directe avec Internet. Il est à noter que le Smart-Phone peut également se connecter à Internet en utilisant le réseau GSM. Cependant, pour la majorité des opérateurs, cet accès utilise également la technologie NAT, gérée cette fois-ci par l'opérateur.

1.2.4.2 Effet passerelle

Le réseau sur lequel un équipement connecté reçoit ses services traditionnels, tels qu'une émission télévisée ou le réseau téléphonique, utilise ses propres protocoles et son propre mode de fonctionnement. L'adjonction d'une connexion Internet à un équipement incite les fabricants à exploiter de nouvelles fonctionnalités alliant ces deux connexions.

Sur la Figure 1.3, sont représentés deux exemples concrets d'équipements "bi-connectés". D'un coté, le Smart-Phone, relié à la fois au réseau de "service distant",

le réseau GSM, et au réseau WiFi le reliant à Internet. De l'autre coté, la Smart-TV, reliée à la fois au réseau de "service distant", qui lui fournit les émissions télévisées, et au réseau local la reliant à Internet et à d'autres équipements du domicile.

1.3 Sécurité des équipements connectés

Comme nous venons de le montrer, les équipements connectés sont désormais très nombreux. Ils prennent de plus en plus de place dans notre société, leur architecture est relativement complexe et leurs possibilités d'interaction vastes. De plus, ces équipements peuvent être amenés à manipuler des informations personnelles des individus, pour lesquelles les propriétés de confidentialité ou d'intégrité peuvent être importantes, en fonction de la nature des informations. On peut donc légitimement se questionner sur la sécurité de ces équipements. Ont-ils été développés avec une réelle prise en compte des problèmes de sécurité ? Ne peuvent-ils pas être des cibles particulièrement intéressantes pour des attaquants ? Ne peuvent-ils pas facilement constituer un vecteur de diffusion massive de maliciels ? La suite de ce chapitre est consacrée à cette problématique. Dans un premier temps, nous revenons sur certaines caractéristiques des équipements connectés afin d'aborder leurs effets positifs ou négatifs sur la sécurité.

Système d'exploitation

Le système d'exploitation et les applications d'un équipement connecté à Internet sont des éléments-clés de sa sécurité. Leur niveau de sécurité est par ailleurs lié à l'application régulière des mises à jour de ceux-ci lorsque des correctifs sont disponibles. Or, les équipements connectés embarquent souvent des logiciels anciens, moins bien maintenus par la communauté [5]. De ce fait, en cas de découverte d'une vulnérabilité concernant un logiciel utilisé, les correctifs tardent généralement avant d'être disponibles. De plus, les fabricants ont souvent du mal à maintenir à jour un système d'exploitation après l'apparition de son successeur, contrairement aux systèmes d'exploitation utilisés par les ordinateurs personnels, dont la durée de maintenance minimale est annoncée à la publication.

Dans la pratique, tout logiciel peut contenir des bugs et être soumis à une évolution de son environnement, nécessitant un correctif. La problématique de maintenir un système à jour par rapport aux failles de sécurité connues peut être un enjeu décisif dans le choix du type de firmware pour un fabricant. En effet, il peut :

— Utiliser un firmware propriétaire et fermé, et ainsi espérer limiter la découverte de vulnérabilités par les attaquants et donc le nombre de correctifs à développer (puisque c'est au propriétaire que reviendra nécessairement la tâche de développer ces correctifs).

5. Pour les objets, comme les micro-capteurs par exemple, n'implémentant pas la pile TCP/IP, il n'y a même pas de connectivité avec Internet lui permettant d'accéder aux mises à jour.

— Utiliser un firmware open-source, dont la disponibilité des sources peut faciliter la recherche de vulnérabilités, mais dont la large diffusion permet de disposer rapidement des correctifs publics.

Il est à noter également que la rapidité de publication d'un correctif suite à la découverte d'une faille peut jouer sur l'image de marque du fabricant.

L'environnement d'un équipement grand public connecté à Internet peut également avoir un impact sur sa sécurité. En effet, son environnement est généralement très différent de celui qui existe dans un environnement professionnel.

Traduction d'adresse

L'utilisation de cette technique [46] présente de nombreux avantages. D'un point de vue de la sécurité, l'avantage principal est que l'UAI devient désormais l'unique équipement visible sur le réseau Internet. Les autres équipements domestiques connectés ne sont pas directement connectés à Internet et de ce fait pas directement accessibles depuis un site distant à travers l'Internet. Ils ne peuvent donc pas être directement attaqués.

Effet passerelle

L'exploitation des technologies d'Internet sur un réseau de services (tels que les services interactifs proposés à l'aide du protocole HbbTV [6] pour les téléviseurs, protocole sur lequel nous reviendrons dans le chapitre 4) nécessite beaucoup de précautions. En effet, ces réseaux de service (réseaux hertziens pour les téléviseurs) ne sont traditionnellement pas considérés comme des sources de menaces. De ce fait, il est souvent plus facile d'injecter des attaques sur ces réseaux et ainsi profiter de l'équipement "bi-connecté" pour atteindre et mettre en péril tout le réseau informatique domestique, en jouant le rôle de passerelle avec son réseau de services distants. Ce sont justement les vulnérabilités des réseaux de service qui seront au cœur des travaux de cette thèse, comme nous le montrerons dans la suite de ce manuscrit.

1.4 Travaux connexes

Alors que très peu d'études s'intéressent de manière générale à la sécurité des équipements connectés, beaucoup de travaux ciblant des attaques particulières existent. Nous présentons ces dernières à travers une classification des attaques dans la suite de cette section. Avant cela, nous présentons dans le paragraphe suivant quelques travaux concernant la sécurité des équipements connectés de manière générale. Ces travaux sont les plus proches des objectifs de cette thèse mais, à notre connaissance, ils sont encore peu nombreux.

6. Hybrid Broadcast Broadband TV.

L'Independent Security Evaluators [50] a mené une étude globale sur les problématiques liées aux UAI grand public. Dans un premier temps, sont abordés notamment les services supplémentaires, comme l'UPNP, fournis et activés par défaut sur ces équipements, ainsi que les vulnérabilités associées. Puis, sont présentées plusieurs attaques en tant que preuves de concept permettant de compromettre ces UAI. Codenomicon [66] met en avant leur solution de fuzzing afin de tester la résistance de différents services d'un ensemble de téléviseurs à des entrées anormales. Durant cette étude les protocoles IPv4, DVB, UPnP, Image, Audio et Video sont testés. Les résultats de cette étude montrent le manque de sécurité dans l'implémentation de ces protocoles. De plus, des protocoles existant depuis longtemps, comme l'IPv4, ne résistent aux tests que dans 3 cas sur 6.

Andrei Costin et al. [35] analysent massivement les firmwares embarqués dans les équipements connectés. Durant leur étude, ils se sont intéressé à 32.000 firmwares, représentant 1,7 millions de fichiers, qu'ils ont analysé statiquement. Les résultats de cette étude mettent en avant l'intérêt d'analyser simultanément plusieurs équipements, permettant de corréler des vulnérabilités entre différents équipements. Dans [39], les auteurs analysent régulièrement des parties d'Internet à la recherche d'équipements embarqués vulnérables. Leur analyse a permis de détecter plus de 540.000 équipements accessibles depuis Internet, configurés avec un mot de passe par défaut, soit plus de 13% des équipements embarqués découverts. De plus, après 4 mois, 96% de ces équipements sont toujours vulnérables. Dans [38], les auteurs mènent des études similaires. Ils estiment la probabilité qu'un équipement grand public soit vulnérable est de 45.62%, contre 2.46% pour les équipements professionnels. Dans [27], les auteurs vont plus loin en déployant systématiquement leur application d'analyse lorsqu'ils trouvent une machine vulnérable, i.e. utilisant un mot de passe par défaut. Ils ont arrêté leur analyse après avoir déployé plus de 30.000 fois leur binaire. Cette étude montre à quel point il est facile de mettre en place aujourd'hui une attaque distribuée. Enfin, dans [77], les auteurs analysent chaque adresse IPv4 routable sur Internet à la recherche d'équipements répondant à une requête de découverte UPnP. Il s'avère que plus de 81 millions d'adresses IP répondent, dont plus de 69% utilisent une version vulnérable d'UPnP.

1.4.1 Critères de classification des attaques

La suite de cette section est destinée à proposer une classification des attaques existantes ciblant les équipements connectés à Internet. Ici, nous présentons d'abord les critères que nous avons utilisés pour cette classification.

Dans la section 1.2.4, nous avons abordé l'environnement d'un équipement grand public connecté à Internet. Dans le Tableau 1.1, nous avons mis en avant les différentes E/S d'un équipement connecté et leurs propriétés. Ces différentes caractéristiques nous ont permis d'établir trois hypothèses autour desquelles s'oriente notre classification comme représentée dans la Figure 1.4 :

— l'attaquant est l'utilisateur lui-même, il possède un accès physique à l'équipement.

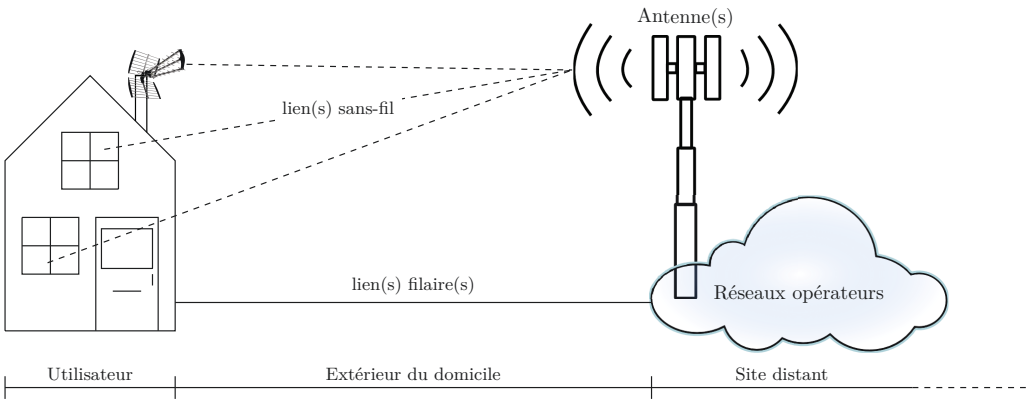


FIGURE 1.4 – Rayons d'attaque

— l'attaquant est sur un site distant et tente d'accéder à l'équipement à travers Internet. L'attaquant peut exploiter des failles dans le logiciel de l'équipement lui-même ou peut tenter d'installer indirectement des applications malveillantes (virus, plugins, mises à jour, etc.) dans l'équipement, par exemple en déposant ces applications malveillantes sur les serveurs de dépôt de l'équipement.
— l'attaquant se situe à l'extérieur du domicile et tente d'accéder à l'équipement en intervenant physiquement sur l'un des réseaux connectant le domicile aux fournisseurs de services et d'accès à Internet.

Pour chaque hypothèse, nous différencions l'attaque selon son impact en terme de sécurité, selon les trois attributs définissant la sécurité-immunité dans la sûreté de fonctionnement : disponibilité, intégrité et confidentialité, définis dans la section 1.1.1.

1.4.2 Attaques depuis le domicile

Le domicile de l'utilisateur étant considéré "sûr", les attaques perpétrées depuis le domicile sont donc réalisées par l'utilisateur lui-même. Ceci a un impact sur les motivations de l'attaquant, qui cherche en général à étendre ses privilèges ou à accéder à des services auxquels il n'a pas souscrit. En conséquence, ce type d'attaque va principalement nuire aux intérêts du fabricant ou du fournisseur de services correspondant à l'équipement ciblé.

1.4.2.1 Disponibilité

Les attaques depuis le domicile ciblant la disponibilité semblent très peu vraisemblables. En effet, rendre son propre équipement indisponible, ne nuit ni au fabricant, ni au fournisseur de service de l'équipement en question, ni a priori aux autres utilisateurs. Cette attaque, qui consisterait en fait pour un attaquant à se pénaliser uniquement lui-même, ne semble pas avoir de sens. Cependant, de plus en

plus de fournisseurs offrent la possibilité de configurer son propre UAI en hotspot WiFi afin de mettre à disposition sa connexion Internet aux utilisateurs du même FAI, passant à proximité du domicile. Dans ce cas, on peut imaginer une attaque contre la disponibilité de son propre équipement, pénalisant les autres utilisateurs de l'équipement.

1.4.2.2 Intégrité

Les attaques depuis le domicile ciblant l'intégrité d'un équipement visent généralement à détourner l'usage qui en est initialement prévu. Les attaquants cherchent principalement à ajouter ou activer des fonctionnalités supplémentaires, pour lesquelles ils n'ont pas payé. Il existe de nombreux sites ou forums [7, 3, 1, 2] regroupant les informations permettant de compromettre ce type d'équipements. Généralement, les attaques consistent à modifier le firmware ou à activer des fonctionnalités cachées.

Différentes études s'intéressent à la sécurité des équipements embarqués connectés à Internet. Dans [89], l'auteur s'intéresse à plusieurs scénarios d'attaque intérieures pouvant impacter l'intégrité d'une Smart-TV. Dans un premier temps, l'auteur s'intéresse à la possibilité de modifier le firmware du téléviseur. Ce firmware est chiffré en utilisant des clefs AES [7]. Toutefois, cette protection se révèle insuffisante, car en utilisant des outils fournis par Altinyurt dans [7], l'auteur est capable de déchiffrer le contenu du firmware. Cependant, il n'est pas capable de charger un firmware modifié par ses propres soins, car le téléviseur en vérifie la signature. Dans un second temps, l'auteur s'intéresse à la possibilité de charger des applications malveillantes. Une application créant un accès shell est proposée sur Internet [7] ; cependant un accès physique au téléviseur est nécessaire pour l'installer, car l'application n'est pas signée par le fabricant.

Dans [20] et [21], l'auteur s'intéresse au port série (de service), disponible sur son téléviseur. Dans un premier temps, l'auteur montre que grâce à 1) l'information affichée sur l'interface de debug et 2) l'exploitation d'une vulnérabilité d'un service réseau (traversée de répertoire), il est possible d'extraire le binaire MIPS [8] qui s'occupe des mises à jour de ce téléviseur. Grâce à ce binaire, l'auteur est capable de déchiffrer les mises à jours de ce téléviseur. Puis, dans un second temps, en analysant le trafic réseau sortant, l'auteur découvre la présence d'une librairie UPnP possédant une vulnérabilité documentée. Grâce à la connaissance du firmware et d'informations suffisantes sur le système, l'auteur a été capable de réaliser un débordement de tampon dans la pile permettant d'activer un serveur SSH [9] sur le téléviseur.

Dans [101], les auteurs montrent que les cartes SD contiennent en réalité des microprocesseurs permettant de réaliser les fonctions de correction d'erreur et de gestion de blocs défectueux. De ce fait, même une carte SD contient un firmware

7. *Advanced Encryption Standard* [40]
8. Architecture de processeur : *microprocessor without interlocked pipeline stages.*
9. *Secure Shell*

contenant le code de ces fonctions. En visitant des magasins d'électronique en Chine, les auteurs ont aperçu un vendeur modifiant le firmware, afin d'en étendre la capacité. Il s'est alors intéressé à cette procédure afin d'y insérer son propre code. De cette manière, il est possible d'exploiter un processeur bien plus puissant que celui d'un Arduino [10] par exemple, classiquement utilisé pour ce type de développement, pour un coût bien plus faible.

1.4.2.3 Confidentialité

Les attaques depuis le domicile ciblant la confidentialité visent à récupérer des informations sensibles provenant du fabricant ou de l'un des fournisseurs de services distants de l'équipement en question. L'attaque la plus fréquente, car la plus monnayable, est la divulgation des clefs de chiffrement utilisées par les décodeurs de flux vidéos (*Set-Top Box*) permettant de donner accès aux chaînes payantes uniquement aux détenteurs d'une carte à puce pour laquelle a été payé un abonnement. Les attaquants vendent des équipements modifiés [69] permettant de tirer profit des clefs de chiffrement ainsi partagées.

L'analyse des firmwares d'un équipement connecté est également un vecteur d'attaque fréquemment exploré. En effet, la connaissance du firmware de l'équipement visé permet généralement à l'attaquant d'élaborer son attaque, comme montré précédemment dans [20] et [21]. Dans [56], l'auteur montre comment il est possible de réaliser une attaque MitM ("*Man in the Middle*") sur un lien USB durant une mise à jour, suivant le protocole DFU [11], afin d'extraire le contenu du firmware.

Finalement, l'analyse de trafic sortant sur le réseau local vers Internet, en utilisant des techniques de MitM [82], permet souvent de révéler beaucoup d'informations. De plus en plus, ces connexions sont protégées par le protocole sécurisé SSL (*Secure Sockets Layer*). Cependant, celui-ci nécessite une bonne implémentation, ce qui n'est pas toujours le cas. Dans [89], l'auteur montre comment il est possible d'analyser des communications, d'apparence sécurisées, entre une Smart-TV et son fabricant.

1.4.3 Attaques logicielles depuis l'extérieur du domicile

Les attaques logicielles extérieures au domicile sont réalisées par un tiers. Ces attaques visent à nuire aux intérêts de l'utilisateur ciblé. Ces attaques exploitent des vulnérabilités dans les composants logiciels du système gérant les E/S ayant un périmètre de fonctionnement différent du domicile (cf. Tableau 1.1).

Dans le cadre des équipements grand public, la majorité des équipements sont protégés contre ce genre d'attaques du fait de l'utilisation des techniques de traduction d'adresses (NAT) et de l'utilisation des adresses IP privées, comme nous l'avons décrit précédemment. Cependant, il existe d'autres techniques, comme le *Cross Channel Scripting* (XCS) [26]. Lors d'une attaque XCS, un canal non-Web,

10. `http://www.arduino.cc/`
11. *Device Firmware Upgrade*

i.e., SNMP ou FTP, est utilisé afin d'injecter une attaque *Cross Site Scripting* (XSS) persistante, qui pourra ensuite cibler tout utilisateur qui accède au serveur Web de l'équipement.

1.4.3.1 Disponibilité

Les attaques logicielles ciblant la disponibilité d'un équipement connecté à Internet sont très fréquentes. Ces attaques, également connues sous le nom de "Denial of Service" (DoS) font partie des problèmes de sécurité les plus compliqués à gérer. Les attaques distribuées, dites "Distributed Denial of Service" (DDoS), dont l'impact peut être bien plus important, sont particuliérement dangereuses et efficaces. Une attaque DDoS peut assez facilement épuiser toutes les ressources informatiques et de communication de sa cible [44]. Richard Stallman, notamment, compare les attaques DDoS à une manifestation dans la rue [92], pour l'exemple.

Les attaques DOS consistent souvent à surcharger un service en particulier [64, 75] sur l'équipement ciblé. Envoyer plus de requêtes que l'application peut gérer pendant un laps de temps suffisamment important, a généralement pour effet de bloquer, redémarrer ou arrêter le service, et parfois même le système.

Il est également possible de rendre indisponible un service en exploitant une vulnérabilité dans celui-ci de façon à le faire défaillir. C'est le cas par exemple du fameux "Ping of Death", qui exploite une vulnérabilité dans certaines implémentations de la pile TCP/IP en envoyant des pings avec plus de 65536 octets de données au lieu des 64 octets habituels [63].

1.4.3.2 Intégrité

Les attaques logicielles ciblant l'intégrité d'un équipement connecté à Internet, visent à altérer le fonctionnement prévu de l'équipement. Ce type d'attaque permet à l'attaquant d'exploiter l'équipement afin de mettre en œuvre d'autres attaques. Les UAI constituent une cible parfaite pour ces attaques, puisqu'elles gèrent la traduction d'adresse et la sécurité d'un réseau domestique ; or ces équipements sont généralement insuffisamment protégés [86, 72].

Ces attaques exploitent généralement une mauvaise protection des interfaces de configuration et de mise à jour. Premièrement, certains fabricants installent des portes dérobées ("*backdoors*") dans les interfaces de configuration de leurs équipements. Dans [87] et [58], les auteurs expliquent comment il est possible d'exploiter ces portes dérobées qu'ils ont découvertes dans des routeurs grand public. Deuxièmement, de nombreux utilisateurs utilisent des mots de passe par défaut. Dans [93], l'auteur montre comment un site contenant du code JavaScript est capable de tenter une modification des paramètres DNS de l'UAI à chaque passage d'un utilisateur sur son site. Finalement, il existe de nombreux équipements connectés directement à Internet, i.e., sans passerelle NAT, proposant des interfaces de mise à jour non sécurisées par un mot de passe. Dans [62], l'auteur montre notamment comment il est possible de changer le firmware d'une imprimante connectée à Internet avec une adresse IP publique.

1.4.3.3 Confidentialité

Les attaques logicielles ciblant la confidentialité d'un équipement connecté à Internet, visent à récupérer des informations personnelles et confidentielles de l'utilisateur ciblé. Pour cela, l'attaquant cherche à obtenir un accès sur le réseau local de l'utilisateur ciblé. Nous considérons toujours le domicile comme "sûr". Le protocole WiFi n'est pas limité par le domicile et est accessible depuis l'extérieur. Ce protocole est généralement protégé par des mécanismes de chiffrement et d'authentification. Dans [83], les auteurs montrent comment certains fabricants utilisent une dérivée de l'adresse MAC de l'équipement comme clef pour protéger le WiFi, ce qui permet, pour un attaquant, de restreindre l'espace possible des clés à parcourir pour une attaque de type brute-force. Plus globalement, les mécanismes de protection de réseaux WiFi se révèlent insuffisants car souvent mal implémentés ou configurés [95, 24, 97]. Finalement, dans [55], les auteurs montrent qu'en utilisant des analyses statistiques, il est possible de déduire la page HbbTV demandée par une Smart-TV en analysant un signal WiFi chiffré, et ainsi divulguer la chaîne TV regardée.

1.4.4 Attaques physiques depuis l'extérieur du domicile

Les attaques physiques extérieures au domicile sont réalisées par un tiers. Ces attaques visent à nuire aux intérêts de l'utilisateur ciblé et éventuellement à celui du fournisseur de service. Ces attaques exploitent des vulnérabilités dans les composants logiciels du système gérant les E/S ayant un périmètre de fonctionnement différent du domicile (cf. Tableau 1.1), en s'interposant physiquement sur l'un des liens de communication entre l'équipement et ses fournisseurs de services ou d'accès à Internet. Ces attaques sont moins fréquentes car elles nécessitent plus de moyens et une proximité plus importante avec la cible.

1.4.4.1 Disponibilité

Les attaques physiques ciblant la disponibilité d'un équipement connecté à Internet peuvent se diviser en deux catégories. D'un coté, les attaques visant les connexions filaires, qui consistent à sectionner le lien afin d'interrompre la communication et ainsi générer une indisponibilité du lien de communication. Ces attaques ne nécessitent pas de technique particulière et sont généralement qualifiées de vandalisme. D'un autre coté, les attaques visant les connexions sans-fil, qui consistent à brouiller le signal afin d'interrompre la communication et ainsi rendre une bande de fréquence indisponible. Malgré une législation stricte en France [13] et dans de nombreux pays, des équipements clef en main existent permettant de réaliser ce type d'attaque [70].

1.4.4.2 Intégrité

Les attaques physiques ciblant l'intégrité d'un équipement connecté à Internet, visent à altérer le fonctionnement prévu de l'équipement, et permettre ainsi à l'attaquant d'exécuter du code malveillant. Ces attaques consistent donc à injecter du code malveillant sur le lien connectant l'équipement à son fournisseur de service ou d'accès à Internet, permettant ainsi de compromettre l'intégrité de l'équipement destinataire de ces données. Dans [76], les auteurs montrent comment simuler une antenne-relais UMTS [12] (3G). Ce type d'attaque nous semble particulièrement intéressant et encore peu exploré. C'est la raison pour laquelle nous nous intéresserons plus particulièrement à ce type d'attaque dans le cadre des cas d'études de cette thèse, que nous décrirons en détail dans les prochains chapitres de ce manuscrit.

1.4.4.3 Confidentialité

Les attaques physiques ciblant la confidentialité d'un équipement connecté à Internet, visent à récupérer des informations personnelles et confidentielles de l'utilisateur ciblé, ainsi que des informations sensibles du fournisseur de service ou d'accès à Internet. Ces attaques peuvent se diviser en deux catégories. D'un coté, les attaques visant les connexions sans-fils, qui consistent à installer et configurer sur le bon canal de communication un équipement correspondant à la technologie utilisée par le lien visé. D'un autre coté, les attaques visant les connexions filaires, nécessitant un équipement particulier permettant d'éviter les phénomènes d'écho. En effet, les liens filaires sont principalement de type "point-à-point" entre deux équipements. Ces attaques, tout comme les attaques visant l'intégrité avec lesquelles elles ont beaucoup de points communs, sont aujourd'hui encore très rares et peu documentées. Nous nous y intéresserons donc particulièrement dans le cadre de nos travaux dans les chapitres suivants.

1.5 Contributions de la thèse

Les sections précédentes décrivent le contexte des équipements grand public et leur évolution avec l'arrivée d'Internet. La démocratisation des équipements connectés à Internet dans les foyers, avec l'utilisation de protocoles limitant la connaissance technique requise pour l'installation de ces équipements, met en risque l'utilisateur final. Des études mettent clairement en avant l'écart concernant la présence de vulnérabilités entre les équipements professionnels et les équipements grand public [38]. Les équipements professionnels commencent à bénéficier de schémas de certification, permettant de s'assurer d'un certain niveau de sécurité. Des volontés d'adapter certains de ces schémas aux équipements grand public existent. Le schéma CSPN [13] est adapté, et commence à être mis en place pour les STB [14] [6].

12. Universal Mobile Telecommunications System
13. Certification de Sécurité de Premier Niveau
14. *Set-Top Box*, décodeur TV.

Ce schéma d'évaluation est issu du groupe de travail *Security Evaluation Methodology for Set-Top boxes* (SEMS) sur la base d'un document rédigé par Sogeti pour Canal+. Ce groupe de travail regroupe différents industriels dont Thales Communications & Security. Il est principalement destiné à évaluer la sécurité des logiciels contenus dans les terminaux permettant la réception de *Pay-TV*[15], mais peut servir de base méthodologique pour d'autres équipements tels que les UAI.

L'analyse de sécurité des équipements grand public est au cœur de cette thèse. Notre objectif est de contribuer à l'analyse des vulnérabilités dans ce type d'équipements. Nous allons pour cela proposer une méthode systématique, fondée sur trois grandes étapes :

- Dans un premier temps, il est essentiel de réaliser une analyse des risques de l'équipement en question. Ces méthodes, pour la plupart issues du monde industriel, permettent d'obtenir une vue globale de l'équipement et de ne négliger aucun risque. Dans le chapitre 2, nous comparons les différentes méthodes existantes avant de détailler celle que nous avons retenue pour nos cas d'étude, la méthode EBIOS.
- Dans un second temps, nous proposons une phase d'expérimentations. Dans le cadre de l'évaluation des liens de communication, nous proposons une méthode en trois étapes afin d'aborder chaque risque identifié :
  - **Observation** : Il s'agit d'observer les communications sur le lien ciblé. Cette étape est très importante car elle permet de s'approprier le protocole utilisé et ses éventuelles particularités.
  - **Simulation** : La seconde étape consiste à développer une plateforme permettant de simuler un environnement de fonctionnement légitime. Ceci permet de s'assurer d'avoir mis en œuvre toutes les particularités du protocole, attendu par l'équipement.
  - **Conduite d'attaque** : La dernière étape consiste à exploiter la plateforme mise en place afin d'injecter des fautes, susceptibles de compromettre l'équipement visé.
- Enfin, il est primordial de concevoir et de proposer des contre-mesures aux faiblesses identifiées dans les équipements analysés.

Cette méthode constitue la première contribution de cette thèse. Nous avons mis en œuvre cette méthode dans deux cas d'étude.

1. Premièrement, nous avons étudié les Unité d'Accès Intégrées, qui sont aujourd'hui au centre de chaque réseau domestique. L'analyse des risques que nous avons menée sur ces équipements nous a conduit à analyser la sécurité de la boucle locale. L'analyse de ce dernier point nous a conduit à développer deux plateformes, la première permettant d'observer toutes les communications sur une boucle locale, la seconde permettant de simuler le comportement d'un Fournisseur d'Accès à Internet.
2. Dans un second temps, nous avons étudié les téléviseurs connectés, également connus sous le nom de Smart-TV. L'analyse des risques que nous avons me-

15. Télévision payante.

née sur ces équipements nous a conduit, entre autres, à étudier la sécurité du flux DVB, et en particulier la sécurité du protocole HbbTV. Les expérimentations correspondantes nous ont conduit à mettre en œuvre une plateforme d'émission DVB.

Les différentes expérimentations techniques réalisées, à travers ces deux cas d'étude, focalisent sur les cas où l'attaquant se situe à l'extérieur du domicile et tente d'accéder à l'équipement en intervenant physiquement sur l'un des réseaux connectant l'équipement à ces fournisseurs de service. Ainsi, ces deux cas d'études visent à apporter une contribution là où il existe aujourd'hui encore un manque d'étude. La présentation détaillée de ces deux cas d'études, des plateformes permettant de réaliser les expérimentations et la démarche d'analyse qui nous a permis, pour chaque cas, de mettre en évidence des vulnérabilités, constituent la seconde contribution de cette thèse.

Dans la suite de ce manuscrit nous présentons d'abord la méthode globale proposée, avant de procéder aux deux cas d'étude. Enfin, nous terminons par étudier les différentes contre-mesures possibles face aux problèmes de sécurité identifiés.

Chapitre 2

Méthode d'analyse

Sommaire

Ce chapitre présente la méthode d'analyse que nous proposons et avons utilisée dans cette thèse. Il est aujourd'hui très difficile d'utiliser les différents équipements connectés en ayant une bonne connaissance des risques que l'on prend en les intégrant à une infrastructure existante dans la sphère professionnelle, mais aussi dans la sphère privée. Pourtant, différentes méthodes d'analyse des risques existent et pourraient être systématiquement utilisées pour évaluer la sécurité de ces différents équipements. La méthode d'analyse générale que nous proposons dans cette thèse est représentée dans la Figure 2.1. La première partie de cette méthode s'appuie sur des méthodes existantes. La rigueur de ces méthodes issues du monde industriel permet d'obtenir une vue des risques associés à l'équipement étudié de manière systématique. C'est pourquoi, le déroulement d'une analyse des risques, constitue la première étape de notre méthode, afin d'identifier les risques et les scénarios de menaces auxquels l'évaluateur doit se consacrer principalement lors de la seconde partie de cette méthode.

Dans la mesure où nous nous intéressons dans cette thèse aux équipements connectés, et en particulier aux problèmes de sécurité impliquant des communications entre l'équipement et son environnement, nous allons nous focaliser plus particulièrement, parmi les scénarios de menaces exhibés à la suite de cette analyse des risques, sur ceux qui vont cibler les communications. Ainsi, la seconde partie de notre méthode est particulièrement centrée sur ce type de menaces et consiste à élaborer des scénarios d'attaque relatifs à ces menaces. Ces attaques mettent en œuvre l'équipement lui-même, dans un environnement opérationnel. Cette seconde étape de notre méthode se déroule en 3 phases :

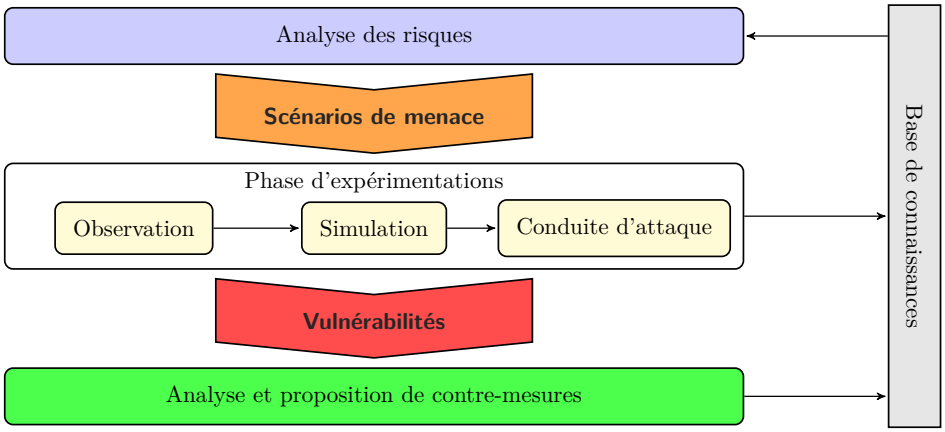


FIGURE 2.1 – Méthode générale proposée

1. **Observation** : Il s'agit dans un premier temps d'observer le fonctionnement légitime du sous-système étudié (ce sous-système est en général un service particulier de l'équipement connecté, associé à l'interface physique qui lui permet de fournir ce service). Cette étape est importante, elle permet de déduire le fonctionnement légitime du service et ses éventuelles particularités.

2. **Simulation** : La deuxième phase consiste à développer une plateforme permettant de simuler le fonctionnement légitime de l'environnement interagissant avec le service visé. Ceci permet de s'assurer d'avoir mis en œuvre toutes les particularités de l'environnement permettant à l'équipement de rendre son service.

3. **Conduite d'attaque** : La dernière phase est dédiée à utiliser la plateforme mise en place dans la seconde phase afin d'injecter des fautes, par la réalisation d'attaques susceptibles de compromettre le service de l'équipement visé.

Nous insistons sur le fait que cette seconde partie est spécifique pour l'évaluation des liens de communication et qu'il est possible qu'elle varie selon le type de scénario de menace étudié. Enfin, dans la troisième partie, nous analysons les contre-mesures efficaces par rapport aux vulnérabilités identifiés. D'une manière générale, ces deux dernières parties servent à alimenter la base de connaissances de l'évaluateur, lui permettant ainsi d'améliorer son analyse des risques. Dans un premier temps, nous allons présenter les différentes méthodes d'analyse des risques existantes avant de nous concentrer sur celle qui a finalement été choisie et utilisée. Ensuite, nous abordons plus en détail les 3 étapes permettant la mise en œuvre des attaques correspondant aux scénarios de menaces identifiés à l'aide de l'analyse des risques.

2.1 Analyse des risques

Une analyse des risques est une méthode permettant d'apprécier et de traiter des risques concernant un domaine d'activité identifié. Le risque est la vraisemblance (plus ou moins grande) de voir un événement, ciblant un bien et exploitant une ou plusieurs vulnérabilités, se réaliser en entraînant des impacts sur un ou plusieurs biens et des conséquences pour le système considéré (cf. Figure 2.2).

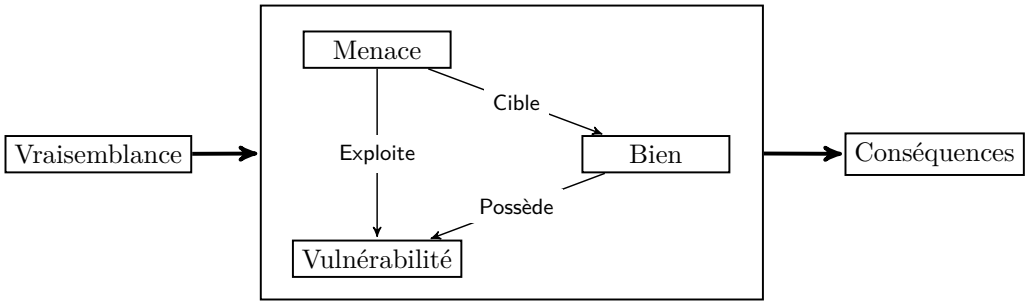


FIGURE 2.2 – Modélisation du risque

Les domaines auxquels peuvent s'appliquer une analyse des risques sont très nombreux et peuvent couvrir des activités très variées. Ils ne concernent pas uniquement la sécurité des systèmes d'information. D'autres domaines, comme la finance ou la médecine, sont également concernés par les analyses des risques. Bien que différentes méthodes existent depuis de nombreuses années, leur encadrement par des normes n'est que très récent. Dans cette section, nous allons dans un premier temps aborder succinctement les normes qui encadrent ce domaine. Plus précisément, nous allons tout d'abord présenter brièvement la norme ISO 31000, qui est la norme la plus générique concernant l'analyse des risques. Ensuite, nous présenterons la norme ISO 27001, qui n'est pas une norme d'analyse des risques à proprement parler, puisqu'elle concerne la gestion de la sécurité des systèmes d'information. Elle est importante dans le contexte de notre étude puisqu'elle concerne justement nos travaux de recherche et parce qu'elle préconise l'utilisation de méthodes d'analyses des risques pour la gestion de la sécurité des systèmes d'information. Après avoir donné un aperçu de ces normes, nous présentons, dans un second temps, une sélection de méthodes d'analyse des risques fréquemment utilisées dans le domaine de la sécurité des systèmes d'information.

2.1.1 Les différentes normes

2.1.1.1 La norme ISO 31000

Du fait des nombreux domaines d'application sur lesquels peut porter une analyse des risques, un ensemble de principes et de lignes directrices génériques, permettant de gérer toute forme de risque, sont réunis dans la norme ISO 31000 [61]. Cette norme est spécifiquement consacrée à la définition des concepts généraux

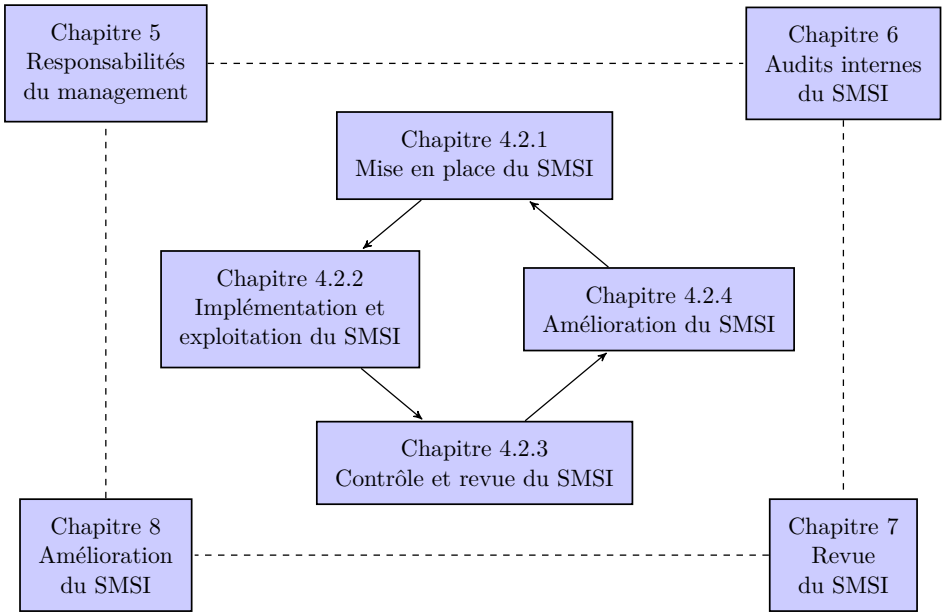


FIGURE 2.3 – Structure de la norme ISO 27001

d'une analyse des risques. C'est pourquoi, comme il est expliqué dans l'introduction de cette norme, elle n'est pas destinée à être utilisée directement à des fins de certification.

La norme ISO 31000 fournit un cadre organisationnel pour la mise en œuvre et le pilotage de la gestion du risque. Elle préconise une approche globale des risques de façon à garantir que le risque est géré de manière cohérente et efficace. Pour cela, cette norme aborde les différents principes de pilotage du risque, que sont la `Politique`, les `Rôles et responsabilités`, la `Communication`, la `Documentation` et le `Contrôle et révision`. De plus, elle définit les 3 principaux buts d'une analyse des risques :

1. Identification des risques
2. Priorisation des risques
3. Traitement des risques

Ainsi, le respect de la norme ISO 31000 permet d'établir un processus de pilotage des risques favorisant le succès du processus de gestion des risques.

Dans le cadre de cette thèse, nous nous intéressons bien sûr au problème de la sécurité et de l'analyse des risques des systèmes d'information (SSI). L'analyse des risques et les méthodes associées dans le domaine de la SSI sont réunies et structurées dans la norme ISO 27001, qui est la norme de référence concernant la gestion de la sécurité des systèmes d'information. Elle va bien au-delà de l'analyse des risques mais cette dernière est une partie incontournable de cette norme. Nous donnons dans la section suivante un aperçu de cette norme.

2.1.1.2 La norme ISO 27001

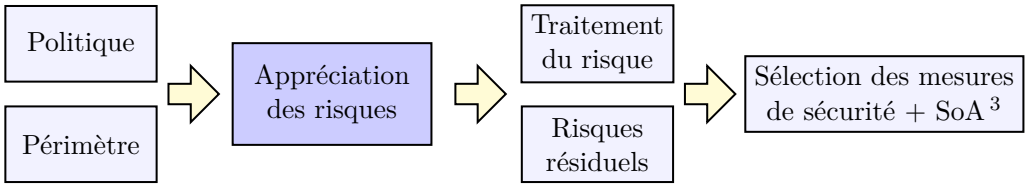
La norme ISO 27001 est la référence des Systèmes de Management de la Sécurité de l'Information (SMSI) [51]. Un SMSI permet d'orchestrer et d'optimiser les différentes mesures de sécurité d'un organisme. La structure de cette norme peut être représentée par la figure 2.3. Le cœur du SMSI est constitué, comme tout système de management ISO, de quatre phases selon la roue de Deming [1], ce qui représente la philosophie générale de cette norme : permettre une amélioration permanente. Le concept d'évolution suivant la roue de Deming sera détaillé davantage dans la présentation de la norme ISO 27005 (cf. section 2.1.2.1).

L'analyse des risques est abordée plus précisément dans le chapitre 4.2.1 de cette norme, qui présente la phase *plan* du SMSI. Cette phase a pour but de définir les procédures nécessaires à la mise en place du SMSI, et se découpe en quatre étapes représentées dans la figure 2.4. C'est la deuxième étape de cette phase qui concerne l'appréciation des risques, qui nous intéresse tout particulièrement dans le cadre de cette thèse [2]. La norme spécifie qu'il est obligatoire, dans le cadre d'un SMSI, d'adopter une méthode d'appréciation des risques. Sans en spécifier une en particulier, la norme définit les sept étapes clefs d'une appréciation des risques :

1. **Identifier les actifs** : Identifier chaque élément d'information important que l'on cherche à protéger, appelé *bien*, au sein du périmètre du SMSI.
2. **Identifier les personnes responsables** : La norme impose la désignation d'un responsable pour chaque bien, en le distinguant clairement du propriétaire.
3. **Identifier les vulnérabilités** : Une vulnérabilité est une propriété intrinsèque du bien qui l'expose à des menaces.
4. **Identifier les menaces** : La menace est l'exploitation d'une vulnérabilité du bien.
5. **Identifier les impacts** : L'impact se définit comme la conséquence de la perte de tout ou partie d'un bien.
6. **Évaluer la vraisemblance** : Remettre les biens dans leur contexte, en tenant compte des mesures de sécurité existantes, afin d'évaluer la vraisemblance des menaces. Par exemple, le vol d'un téléphone portable est bien plus probable que le vol d'un *mainframe* qui bénéficie de la sécurité physique assurée par le bâtiment.
7. **Estimer les niveaux de risque** : Évaluer le niveau de risque final pour chaque bien, compte tenu des informations obtenues lors des étapes précédentes. Il s'obtient en considérant la vraisemblance et l'impact.

1. La roue de Deming est un concept bien plus ancien, issu de l'univers de la qualité du logiciel. La dernière version de la norme ISO 27001 (2013) ne fait plus directement allusion à la roue de Deming, elle utilise la formulation "établir, implémenter, maintenir, améliorer".

2. Les autres étapes, concernant le traitement des risques, ne constituent pas le cœur de ces travaux, mais sont bien sûr très importantes et seront abordées dans le dernier chapitre de ce manuscrit.



3. *Statement of Application*, déclaration d'applicabilité.

FIGURE 2.4 – Les quatre étapes de la phase plan

Afin d'être conforme à la norme ISO 27001, toute méthode d'analyse des risques doit respecter ces sept points. La section suivante présente un certain nombre de méthodes d'analyse des risques parmi les plus courantes, permettant de guider un évaluateur dans la réalisation de ces tâches.

2.1.2 Méthodes d'analyse des risques pour les systèmes d'information

Il existe plusieurs méthodes permettant de réaliser une analyse des risques en SSI. Ces méthodes sont le fruit de travaux étatiques ou d'entreprises privées. Avant de présenter la méthode EBIOS, que nous avons utilisée dans le cadre de cette thèse, nous présentons brièvement cinq autres méthodes, fréquemment rencontrées dans ce domaine.

En plus de ISO 27005 qui est la méthode d'analyse des risques normalisée, nous avons choisi de présenter des méthodes qui sont d'origines différentes et qui présentent des particularités spécifiques. En effet, les différentes méthodes européennes, comme MEHARI *(France)*, EBIOS *(France)* ou CRAMM *(UK)* présentent toutes de fortes similarités. Cependant, MEHARI, contrairement à EBIOS et CRAMM, a été conçue par une association privée et non une entité étatique. Enfin, nous aborderons, OCTAVE, une méthode américaine qui présente une structure bien différente des méthodes européennes.

2.1.2.1 ISO 27005

La norme ISO 27005 [4] est une méthode d'analyse des risques normalisée, ce qui lui permet d'être reconnue internationalement. Cette norme définit les lignes de conduite d'une appréciation des risques et le traitement de ces risques dans le cadre des systèmes d'information [74]. Avant l'apparition de cette norme, il existait déjà de nombreuses méthodes d'analyse des risques. La norme ISO 27005 est intéressante dans la mesure où elle apporte un côté itératif à la démarche d'analyse et elle se veut, de plus, pragmatique et accessible. Elle ne s'applique pas uniquement aux SI, mais également à d'autres systèmes, comme les systèmes embarqués par exemple. L'une des principales caractéristiques de cette méthode est de permettre une évo-

4. Cette norme a été revue en mars 2011 suite à la révision d'EBIOS en 2010.

lution constante des résultats. Cette évolution se fonde sur la roue de Deming (cf. Figure 2.5), dans un but d'améliorer continuellement l'état de sécurité du système :

1. **Plan** : Identification des risques, évaluation des risques et définition des actions de réduction des risques.
2. **Do** : Exécution de ces actions.
3. **Check** : Contrôle du résultat.
4. **Act** : Modification du traitement des risques selon les résultats.

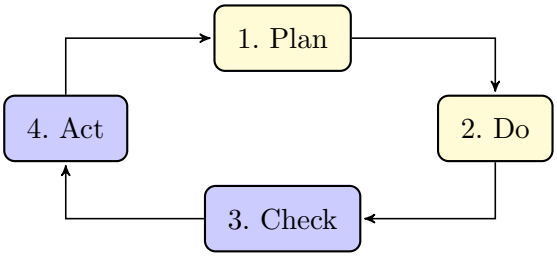


FIGURE 2.5 – Roue de Deming

La norme ISO 27005 définit six étapes :

— **Organisation du processus de gestion des risques** : Définir le périmètre, les objectifs, les critères nécessaires à la gestion des risques et l'organisation associée au processus de gestion des risques.
— **Identification des risques** : Identifier les actifs, les menaces, les mesures de sécurité existantes, les vulnérabilités et leurs conséquences.
— **Mesure de la portée des risques** : Estimer les conséquences, la vraisemblance et la gravité pour chaque risque, afin de préparer leur hiérarchisation.
— **Détermination de l'importance des risques** : Confronter les risques aux critères d'évaluation des risques définis dans le contexte de l'étude, afin de déterminer l'importance des risques et de les ordonnancer.
— **Sélection des solutions** : Sélectionner et proposer des solutions pour réduire, maintenir, contourner ou transférer les risques.
— **Prise de décisions** : Confirmer ou infirmer le choix de traitement des risques de l'étape précédente.

2.1.2.2 MEHARI

La méthode MEHARI (Méthode harmonisée d'analyse des risques) a été créée en 1996 par l'association CLUSIF [5] (Club de la sécurité de l'information français) [33]. Le CLUSIF est un club professionnel, constitué en association indépendante loi 1901, ouvert à toute entreprise ou collectivité. Il est destiné à agir pour la sécurité de l'information et entend sensibiliser tous les acteurs en intégrant une dimension

5. `https://www.clusif.asso.fr/`

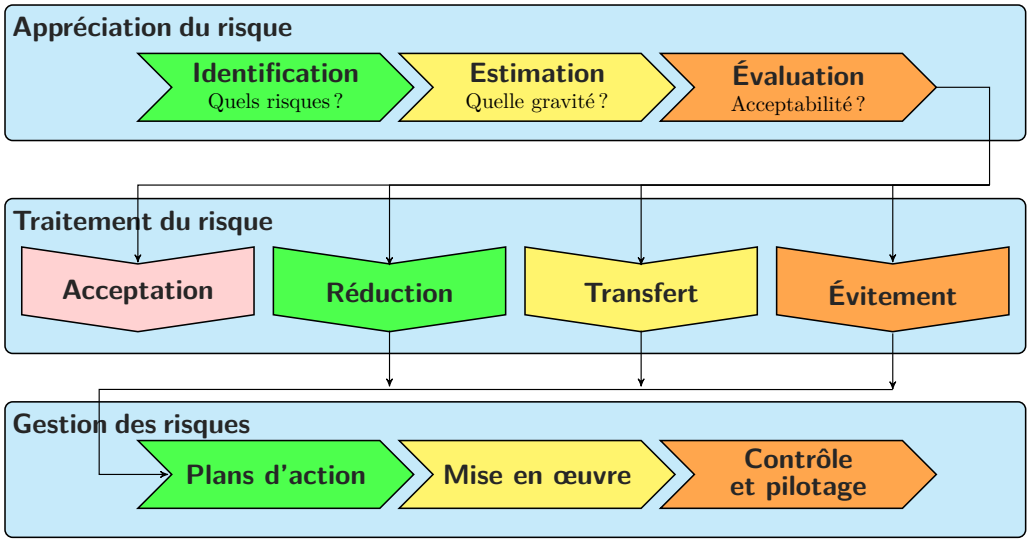


FIGURE 2.6 – Méthode MEHARI

transversale dans ses groupes de réflexion comme la gestion des risques, le droit ou l'intelligence économique.

La dernière version de MEHARI a vu le jour en 2010. La méthode MEHARI suit un plan proche de celui décrit dans la norme ISO 27005 en définissant 3 phases :

— **L'appréciation des risques**
— **Le traitement des risques**
— **La gestion des risques**

Ce plan et ces différents aspects sont schématiquement représentés dans la Figure 2.6.

2.1.2.3 CRAMM

La méthode CRAMM (CCTA Risk Analysis and Management Method) a été établie en 1987 conjointement par Siemens et l'état britannique. CRAMM a pour avantage d'être une méthode très rigoureuse, mais également très lourde en parcourant près de 3000 points de contrôle. Cette méthode est composée de 3 principales phases :

— **Identification de l'existant**
— **Évaluation des menaces et des vulnérabilités**
— **Choix des remèdes**

Un des intérêts de cette méthode est qu'elle inclut nativement des bases de données de connaissances et de contre-mesures qui peuvent faciliter l'évaluation.

La démarche générale de cette méthode est définie dans la figure 2.7.

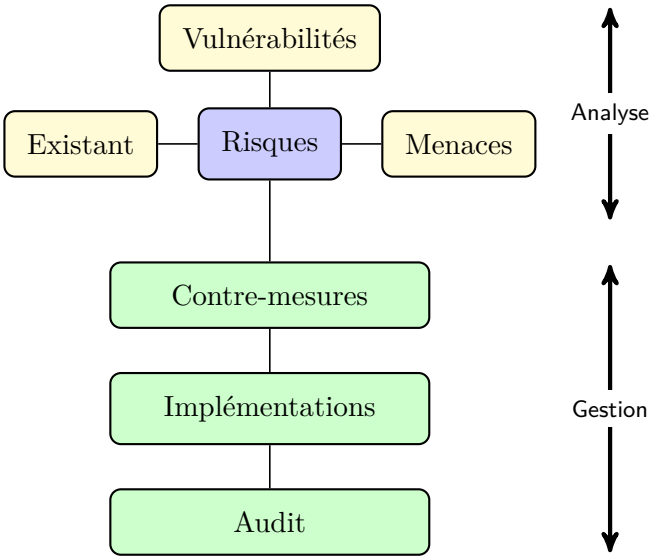


FIGURE 2.7 – Méthode CRAMM

2.1.2.4 OCTAVE

La méthode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) a été élaborée par le CERT du Carnegie Mellon University en 1999 [30]. Contrairement aux méthodes européennes, cette méthode présente une gestion des risques opérationnels d'un côté et une gestion des risques purement informatiques de la DSI de l'autre. On remarque cette différence de philosophie dans la Figure 2.8, qui présente la méthode OCTAVE.

Une analyse OCTAVE se déroule en trois phases :

— **Phase 1** : Identification des biens importants liés à l'information ainsi que les stratégies de protection actuellement utilisées ; puis classification des biens en fonction de leur degré d'implication dans la réussite de l'organisation ; puis définition des exigences de sécurité ainsi que des menaces potentielles.

— **Phase 2** : Évaluation de l'infrastructure du système d'information afin de compléter l'analyse des menaces réalisées lors de la phase 1.

— **Phase 3** : Identification des risques et élaboration d'un plan d'atténuation des risques concernant les biens critiques.

2.1.2.5 EBIOS

La méthode EBIOS [5] (Expression des Besoins et Identification des Objectifs de Sécurité) a été créée en 1995 par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). La dernière version (2010) a été élaborée en collaboration avec le Club EBIOS [6]. La figure 2.9 présente la démarche décrite dans la méthode EBIOS. Conforme aux normes ISO 27001 et ISO 27005, elle a le principal avantage

6. Crée en 2006 dans le but de contribuer au développement de la méthode EBIOS.

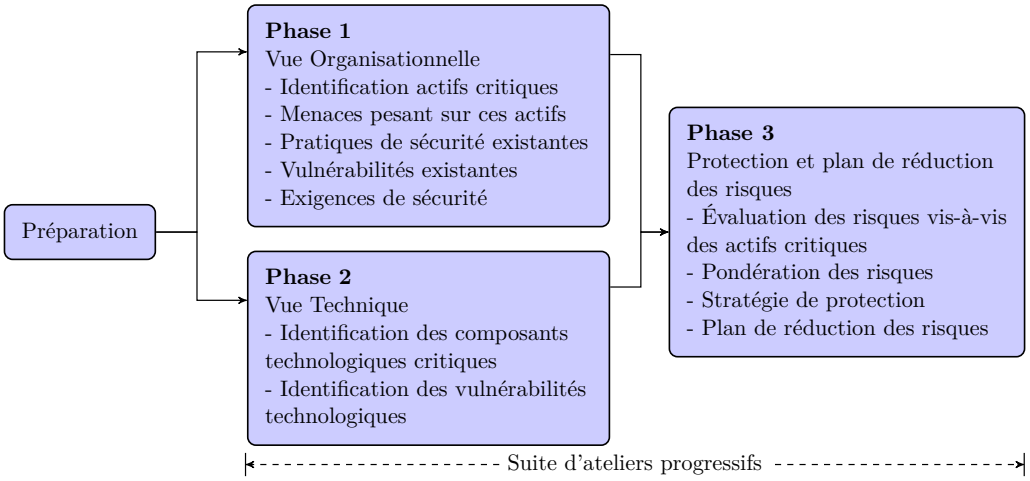


FIGURE 2.8 – Méthode OCTAVE

d'être utilisée en France par une grande majorité d'administrations. En proposant une méthode générique, adaptable à n'importe quel contexte [7] et en incluant une base de connaissances issue de l'expérience, il s'agit d'une méthode clef en main. De plus, la nouvelle démarche EBIOS 2010 se veut itérative, permettant de faire plusieurs fois appel à chaque étape afin d'améliorer progressivement les résultats de l'étude.

Nous présentons ici les 5 modules qui guident une analyse des risques EBIOS.

— **Module 1** : Définition du contexte de l'étude. Ce module est une étape très importante dans la méthode EBIOS. En effet, la définition du contexte peut avoir un impact sur les résultats car on ne considère pas les mêmes besoins de sécurité selon le profil d'utilisateur. On y définit les différentes métriques utilisées ainsi que le périmètre de l'étude. On identifie également les biens essentiels et biens supports ainsi que les mesures de sécurité existantes à prendre en compte dans le traitement des risques. La définition des biens essentiels et biens supports d'un système sert à 1) identifier les fonctions principales réalisées par le système (biens essentiels), et 2) identifier les parties du système permettant de réaliser les fonctions principales (biens supports). Ce module est important pour la réussite de l'analyse des risques et ne doit pas être négligé. En effet, cette réussite dépend non seulement de la maîtrise de la méthode mais également des connaissances de l'environnement étudié.

— **Module 2** : Formulation des événements redoutés en identifiant les besoins de sécurité associés aux biens essentiels ainsi que les impacts en cas de non respect de ces besoins. Il identifie également les sources de menaces susceptibles d'en être l'origine.

— **Module 3** : Identification des scénarios pouvant engendrer les événements

7. EBIOS est utilisable dans d'autres contextes que la sécurité de l'information.

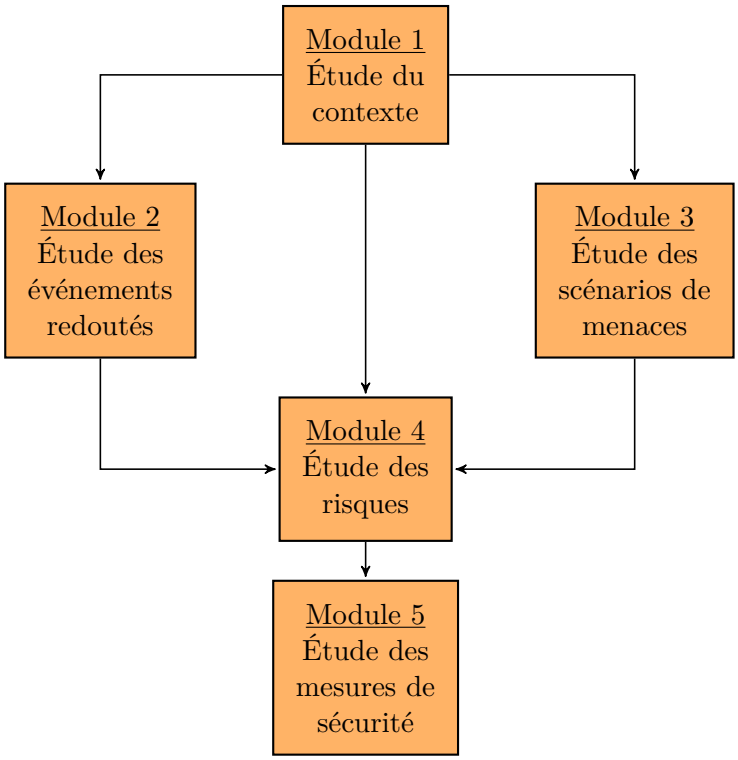


FIGURE 2.9 – La démarche EBIOS

redoutés. Pour cela, ce module étudie les scénarios de menace que peuvent générer les sources de menaces et les vulnérabilités exploitables.

— **Module 4** : Confrontation des événements redoutés aux scénarios de menaces permettant ainsi d'obtenir les différents risques du système.

— **Module 5** : Traiter les risques en proposant des mesures de sécurité à mettre en œuvre.

2.1.3 Identification & appréciation des risques

Dans le cadre de notre méthode d'analyse de la sécurité des équipements grand public connectés à Internet, nous utilisons seulement les parties permettant d'identifier et d'apprécier les risques. Ces parties ont plusieurs intérêts que nous exploiterons dans la suite de notre méthode. Premièrement, l'identification permet d'obtenir une vue de tous les risques liés à l'équipement analysé. Secondement, l'appréciation identifie la vraisemblance et l'impact de chaque risque. Dans les deux cas d'étude que nous présentons dans les chapitres 3 et 4, nous avons mis en œuvre une partie de la méthode EBIOS afin d'identifier les risques associés à l'équipement concerné par l'étude, plus précisément les modules 1 à 4. À l'issue du module 4, nous avons obtenu un tableau classant chaque risque en fonction de sa vraisemblance et de sa gravité. L'étude sur les Unités d'Accès Intégrées dans le chapitre 3 permettra

d'apporter une vue plus approfondie sur les 4 premiers modules de cette méthode.

Nous précisons que nous ne préconisons aucune méthode particulière dans le cadre de nos travaux. Cependant, la méthode utilisée doit permettre à l'évaluateur d'acquérir une vue des différents risques du système, et ceci de manière systématique. Le choix de la méthode EBIOS, dans le cadre de cette thèse, est lié aux multiples avantages qu'elle présente, comme sa base de connaissances ou encore sa généricité. De plus, c'est la méthode privilégiée au sein de Thales Communications & Security, qui est le partenaire industriel de ces travaux de thèse.

2.1.4 Discussion

La conduite d'une analyse des risques est nécessairement une étude subjective. En effet, elle résulte principalement de l'expérience de l'évaluateur, qui doit guider le commanditaire de l'étude. Ainsi, d'une étude à une autre, les besoins et les priorités peuvent être placés différemment, selon le contexte de l'étude.

Dans le cadre de ces travaux de recherche, pour lesquels nous nous plaçons dans une démarche générale et non dans un contexte spécifique, nous avons dû faire des choix sur l'estimation de l'impact des risques étudiés. Comme nous le verrons dans les deux cas d'études présentés dans les deux chapitres suivants, nous avons dû déterminer les risques présentant l'impact le plus important. Les risques que nous avons considérés comme ayant l'impact le plus important sont ceux qui peuvent mener aux dommages les plus importants sur le système considéré. De plus, les risques qui, à notre connaissance, bénéficient de peu d'études de recherche permettant de proposer des contre-mesures nous semblent plus critiques. Ainsi, comme dans tout travail subjectif, il est évident que nous avons fait des choix et que peut-être, les choix auraient été différents dans un autre contexte. Cependant, ceci ne remet en aucun cas en cause la méthode générale que nous proposons dans cette thèse.

De même, une fois les différents risques et leurs impacts identifiés, la seconde phase de notre méthode, présentée dans la section suivante, consiste à étudier expérimentalement chaque scénario de menace associé aux risques identifiés. Dans le cadre de nos travaux, nous n'avons expérimenté que quelques scénarios d'attaques, ceux qui sont associés aux risques à impact maximum et qui concernent les communications des équipements avec leur environnement, en particulier parce qu'ils constituent selon nous des chemins d'attaque originaux peu étudiés jusqu'à maintenant. Ici également, cela ne remet pas en cause une méthode générale fondée sur l'utilisation d'une analyse des risques suivie d'une phase d'expérimentations.

2.2 Expérimentations

Cette seconde étape de notre méthode d'analyse de la sécurité des équipements grand public connectés à Internet, est destinée à démontrer de manière technique, l'existence de vulnérabilités exploitables relatives aux risques sélectionnés lors de

l'étape précédente. Les expérimentations que nous avons menées sont composées de trois phases, présentées et discutées dans les trois sections suivantes.

2.2.1 Observation passive

L'observation passive est sans doute la phase la plus importante. En effet, elle va apporter d'importants atouts à l'évaluateur, cherchant à réaliser une exploitation correspondant à l'un des risques identifiés lors de l'analyse des risques de l'équipement. Cette phase est destinée à acquérir une compréhension technique de l'environnement visé, en analysant les protocoles et/ou applications utilisées. Pour cela, il est nécessaire de mettre en œuvre des techniques d'écoute sur les liens, internes ou externes de l'équipement visé. En réalité, cette phase constitue, en elle-même, une attaque sur la propriété de confidentialité. De ce fait, la mise en œuvre de cette phase va, dans certains cas, nécessiter l'utilisation de techniques particulières. L'observation, correspond principalement aux travaux discutés dans les sections 1.4.2.3, 1.4.3.3 et 1.4.4.3 : les attaques impactant la confidentialité.

2.2.1.1 Observations passives depuis le domicile

Lorsque l'évaluateur est en situation d'utilisateur, il possède un accès physique et, a priori, privilégié à l'équipement et son environnement. Ainsi, les seuls obstacles à la mise en œuvre d'une observation résident dans l'existence de méthodes de chiffrement ou d'obscurcissement prévues par le fabricant. Les E/S (cf. Tableau 1.1) les plus fréquemment exploitées sont les ports USB, série et JTAG. La connectique permettant de se connecter à ces E/S est, la plupart du temps, en vente libre. Des équipements spécialisés, permettant d'opérer en "homme du milieu", existent, mais ils sont souvent très onéreux [8]. Ce type d'observation est déjà largement couvert par un certain nombre d'études (cf. section 1.4.2) et nous avons donc fait le choix de ne pas nous focaliser sur ce type d'observation dans le cadre de cette thèse.

2.2.1.2 Observations passives de l'extérieur du domicile

Lorsque l'évaluateur est en situation d'attaquant extérieur, il doit se contenter des communications sortant du domicile. Dans ce cas, nous distinguons deux cas de figure : les attaques logicielles et les attaques physiques. Dans le cadre des attaques logicielles depuis l'extérieur du domicile, l'observation du comportement de l'équipement analysé devient très compliquée, voire impossible.

En revanche, les attaques physiques depuis l'extérieur du domicile offrent une toute autre perspective. En effet, les liens sortant du domicile sont souvent des liens privilégiés entre l'équipement de l'utilisateur et les fournisseurs de services. De ce fait, les communications sur ces liens ne sont pas observables depuis Internet. Cependant, l'écoute sur ces liens va nécessiter un équipement adapté. Dans le cadre des émissions unidirectionnelles il suffit d'utiliser un équipement homogène

8. Teledyne LeCroy, i.e., fournit des analyseurs de protocole USB, eSATA, etc.

à l'équipement analysé. Dans le cadre d'une communication bidirectionelle, il est souvent nécessaire de développer un équipement au cas par cas. En effet, dans cette situation, il existe souvent une négociation entre les deux protagonistes.

2.2.2 Simulation

La simulation permet à l'évaluateur de s'assurer qu'il est capable de communiquer de manière cohérente avec l'équipement et que celui-ci interprète correctement les données reçues. Il s'agit ici de simuler l'environnement de l'équipement étudié. Cela peut nécessiter l'utilisation de matériel spécifique disposant de l'interface de communication adéquate et l'utilisation d'un logiciel qui doit simuler le service légitime avec lequel l'équipement communique.

Par exemple, lorsque l'évaluateur étudie les vulnérabilités des procédures de mise à jour, il peut envisager d'utiliser l'une des E/S pour altérer ou remplacer le firmware de l'équipement. Ceci permet, par exemple, d'activer des fonctionnalités pour lesquelles l'utilisateur n'a pas payé et ainsi compromettre la propriété d'intégrité de l'équipement. Dans ce cas, il peut être intéressant, dans un premier temps, d'effectuer une tentative de mise à jour avec un firmware légitime, fourni par le fabricant. Ainsi, dans cette première phase, on réalise une simulation du protocole de mise à jour sans injection d'attaque particulière. Elle permet à l'évaluateur de s'assurer qu'il a correctement implémenté le protocole de mise à jour. De plus, pour certains scénarios, la simulation s'avère essentielle lorsque le service ciblé nécessite de répondre correctement à d'autres étapes du protocole avant de pouvoir injecter une attaque.

Cette étape est généralement une approche de type *boîte noire*. En effet, l'évaluateur n'a, a priori, aucune connaissance particulière sur le fonctionnement interne du système qu'il étudie. Toutefois, les résultats de la phase d'observation lui donnent de précieuses informations facilitant cette étape. La méthode que nous proposons pour la mise en place de l'environnement de simulation se déroule en quatre étapes répétées de manière cyclique (cf. Figure 2.10).

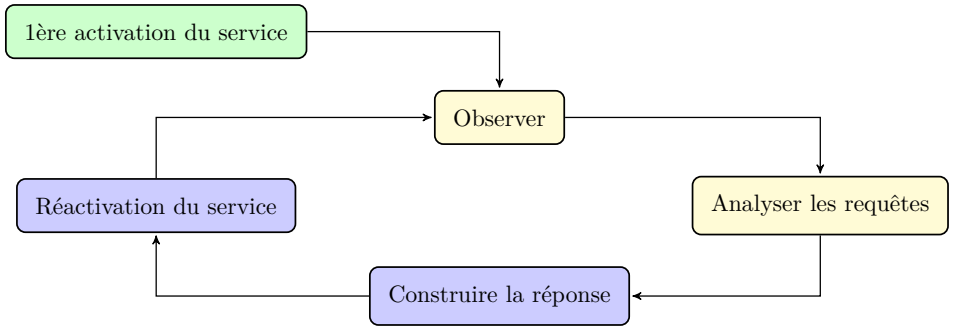


FIGURE 2.10 – Méthode itérative

— **Observer** : après le démarrage du service étudié, nous observons les requêtes émises par celle-ci sur le lien réseau reliant l'équipement à l'opérateur ;
— **Analyser les requêtes** : nous analysons les requêtes qui semblent empêcher l'équipement de poursuivre le démarrage du service étudié. Souvent ces requêtes sont émises à intervalles réguliers en attendant une réponse ;
— **Construire la réponse** : nous installons et configurons les logiciels nécessaires permettant de répondre à la dernière requête reçue ;
— **Réactivation du service** : nous redémarrons l'équipement ou le service de façon à procéder à une nouvelle séquence de démarrage du service étudié.

Ces quatre étapes sont exécutées itérativement jusqu'à atteindre le service visé par l'étude.

2.2.3 Conduite d'attaque

Cette dernière étape consiste à détourner le fonctionnement normal du système. Pour cela, l'évaluateur va injecter des données et/ou configurations malveillantes à l'intérieur de l'environnement de fonctionnement simulé. Conceptuellement, cette étape a des similitudes avec un moteur de fuzzing, qui tente de manière presque aléatoire de modifier les données pour tester le protocole utilisé. En pratique, cette étape est cependant plus ciblée et consiste à injecter du code malveillant spécifiquement destiné à exploiter une vulnérabilité de l'équipement. L'exécution de ce code malveillant peut avoir des objectifs différents, comme l'activation d'une fonction non prévue par le fabricant, la défaillance de l'équipement, ou le vol d'informations. Par exemple, si l'évaluateur a réussi à mettre en œuvre une plateforme de simulation capable de communiquer avec le service de mise à jour de l'équipement, cette étape consiste par exemple à proposer un firmware malveillant à celui-ci.

Il est important de noter que cette étape va conduire l'évaluateur à réaliser des opérations que l'on peut considérer comme illégales. Cependant, elles sont autorisées dans le cadre d'évaluations de sécurité par des centres accrédités par l'ANSSI, tels que le CESTI de Thales Communications & Security ou dans le cadre de travaux de recherches, dans le but d'améliorer la sécurité des équipements étudiés. Les expérimentations réalisées dans le cadre de cette thèse entrent dans ce cadre.

2.3 Conclusion

L'analyse de vulnérabilités des équipements connectés est une vaste tâche pour laquelle il nous a semblé important de proposer une méthode, afin d'organiser au mieux cette analyse et d'optimiser le temps d'analyse. De plus, étant donné la complexité de ces équipements, il semble difficile d'être exhaustif et il est donc important de ne pas partir dans toutes les directions, sans réflexion préalable.

C'est pourquoi, ce chapitre met en avant une méthode qui vise principalement à identifier les différentes menaces qui pèsent sur ces équipements, et à quantifier le risque associé à ces menaces pour l'équipement analysé. Pour cela, nous avons décidé de nous appuyer sur une méthode d'analyse des risques utilisée aujourd'hui.

Après avoir présenté les principales étapes d'une méthode d'analyse des risques, nous avons détaillé quelques méthodes parmi les plus utilisées aujourd'hui et justifié le choix de la méthode que nous avons concrètement utilisée dans nos travaux : la méthode EBIOS. L'intérêt de l'utilisation de la méthode EBIOS est pour nous de pouvoir mettre en évidence les risques les plus importants et de pouvoir se focaliser ensuite sur ces risques particuliers et leurs scénarios de menaces associés.

Une fois ces risques identifiés, la suite de l'analyse consiste à concevoir des expérimentations afin de confirmer ou d'infirmer les risques pressentis lors de l'analyse des risques. Nous avons proposé une méthode d'exploitation de ces vulnérabilités basée tout d'abord sur l'observation. En effet, l'exploitation des vulnérabilités nécessite la compréhension des mécanismes d'entrées/sorties utilisés par l'équipement, mécanismes qui matérialisent les interactions avec l'environnement extérieur, et grâce auxquels des fautes peuvent être injectées. Nous proposons donc d'établir une plateforme permettant, tout d'abord, d'observer ces communications puis, de réaliser nous-mêmes ces communications en simulant l'environnement extérieur puis, finalement, d'injecter des attaques depuis cet environnement simulé.

La méthode que nous proposons dans le cadre de cette étude est destinée à être la plus générique possible permettant d'analyser tous les équipements grand public connectés à Internet. Afin de l'illustrer, nous avons réalisé deux cas d'études suivant cette méthode. Nous présentons ces deux cas d'études dans les chapitres 3 et 4. Pour ces deux cas d'études, différents outils et plateformes ont été nécessaires, dont certains ont requis un paramétrage spécifique. Ces différentes plateformes seront présentées à travers nos deux cas d'études dans les deux chapitres suivants.

Chapitre 3

Cas d'étude 1 : Unité d'accès intégrée & réseau d'accès

Sommaire

Ce chapitre présente le premier cas d'étude de cette thèse, concernant l'unité d'accès intégrée (UAI), plus généralement connue sous le nom de BOX Internet ou BOX ADSL en France, et son réseau d'accès. L'étude de cet équipement est particulièrement intéressant, car il est le cœur de la connexion Internet grand public. De plus, cet équipement présente les caractéristiques discutées dans le chapitre précédent, il est à la fois connecté au réseau domestique et à son fournisseur de service, le fournisseur d'accès à Internet. Enfin, il constitue le passage obligatoire de tous les équipements connectés dans le domicile.

Dans un premier temps, nous déroulons une analyse des risques sur cet équipement et nous montrons comment elle nous a orientés vers l'étude de la sécurité du réseau d'accès. En France, et dans de nombreux pays, le réseau d'accès des UAI, ou boucle locale, utilise souvent la paire de cuivre comme support physique. Historiquement, ce réseau a été installé pour les réseaux téléphoniques commutés publics (RTCP). Aujourd'hui, avec l'arrivée de l'Internet pour tous, ce réseau est utilisé pour bien d'autres services, tels que la télévision ou Internet. Ceci implique

que de nombreuses communications de données, possiblement sensibles, utilisent ce réseau. C'est pourquoi, il devient légitime de considérer la sécurité de ce réseau. La deuxième partie de ce chapitre présente les expériences techniques mises en œuvre afin d'illustrer l'exploration de certaines failles de sécurité.

3.1 Analyse des risques d'une UAI

Dans un premier temps, nous allons suivre la méthode EBIOS décrite dans la section 2.1.2.5. Nous verrons comment cette analyse nous a permis d'identifier un scénario de menace original encore peu exploré [17]. La suite de ce chapitre présente les expérimentations techniques mises en œuvre, visant à exploiter ce risque.

Dans cette étude, nous utilisons régulièrement des termes définis dans la norme EBIOS. Afin que ces termes soient reconnaissables dans ce manuscrit, nous avons choisi de les présenter avec une police de caractères particulière, lors de leur première utilisation : `terme EBIOS`.

3.1.1 Contexte de l'étude

3.1.1.1 Objectifs et cadre de l'étude

Le but de cette analyse est d'identifier les risques associés à l'utilisation des UAI incluses dans les offres "triple play" et de les prioriser par ordre d'importance du point de vue de l'utilisateur. Pour cette étude, nous considérons une utilisation privée de l'UAI, et nous réalisons cette étude du point de vue de l'utilisateur.

Nous nous intéressons uniquement à l'UAI, ou "boîtier modem". La STB (*Set-Top Box*), ou "décodeur télévision", ne fait pas partie de cette étude. D'un point de vue environnement, nous nous limitons à ce qui est accessible à l'abonné ordinaire. Par exemple, d'un point de vue infrastructure, nous nous arrêtons aux frontières de l'habitation, ce qui signifie que l'abonné n'a pas d'accès physique au réseau téléphonique en dehors de ce périmètre.

Dans le contexte des UAI, nous avons retenu les 7 `sources de menaces` présentées dans le Tableau 3.1. Nous avons décidé de ne pas différencier ces sources de menaces selon leur `capacité`, pour simplifier l'étude dans un premier temps [1]. La colonne *Humain* permet de différencier les sources humaines des sources non humaines, par exemple les catastrophes naturelles ou les virus qui ne nécessitent pas l'action immédiate d'un humain. La colonne *Int/Ext* localise la source par rapport au périmètre défini, l'habitation. La dernière colonne, *Malveillant*, distingue les sources malveillantes des sources accidentelles.

1. Classiquement, la méthode EBIOS prévoit 3 niveaux de capacités : Faibles, Importantes et Illimitées. Ces capacités sont établies à partir de différents critères (temps, argent, connaissance, etc...).

Sources de menaces	Humain	Int/Ext	Malveillant
Utilisateur interne malveillant	✓	Int	✓
Personne extérieure malveillante réalisant des attaques sans accès physique	✓	Ext	✓
Personne extérieure malveillante réalisant des attaques avec accès physique	✓	Ext	✓
Abonné	✓	Int	
Opérateur	✓	Ext	
Virus[2]		Ext	✓
Problèmes météorologiques		Ext	

2. Représente tout type de maliciel se propageant de façon autonome.

Tableau 3.1 – Sources de menaces

3.1.1.2 Définition des métriques

Tout au long de l'étude, nous utilisons différentes échelles. En effet, chaque composant du système étudié est évalué en fonction de différents critères de sécurité. Ces critères correspondent aux habituelles propriétés de sécurité : *disponibilité, intégrité* et *confidentialité*. Dans le cadre des UAI, nous avons jugé pertinent, par extension de l'intégrité, d'évaluer également l'intégrité des méta-données, soit l'*authenticité*. Pour chaque critère de sécurité, il est ensuite nécessaire de définir une échelle des besoins. Les quatre critères avec chacune leur échelle respective des besoins sont présentés dans le Tableau 3.2. Il est à noter que ces échelles doivent représenter le besoin et la tolérance de l'utilisateur. Des échelles standards sont proposées dans le référentiel EBIOS, nous nous sommes inspirés de ces échelles pour construire les nôtres.

Dans EBIOS, les risques sont classés en fonction de leur niveau de `gravité` et de `vraisemblance`. Pour obtenir ce classement, on évalue la gravité individuelle de chaque `événement redouté`, ainsi que la vraisemblance de chaque `scénario de menaces` (ces termes seront définis dans les sections suivantes). Les échelles utilisées pour la gravité et la vraisemblance sont présentées dans les tableaux 3.3 et 3.4. Nous avons fait le choix de ces échelles, car nous considérons un usage privé au domicile de l'utilisateur de l'équipement, on considère qu'un événement dont la vraisemblance est minimum se produit une fois par an, qu'un événement dont la vraisemblance est significative se produit une fois par mois et qu'un événement dont la vraisemblance est maximum se produit une fois par jour.

3.1.1.3 Identification des biens

Une analyse des risques, suivant la méthode EBIOS, concerne les `biens essentiels` et les `biens supports`. Les biens essentiels sont des biens immatériels, qui sont à protéger. Les biens supports sont, comme leur nom l'indique, les biens tangibles, qui traitent, stockent et transmettent des informations, supports aux biens essentiels précédemment identifiés. Un système peut également déjà avoir intégré des `mesures de sécurité`. La méthode EBIOS préconise de les identifier,

Disponibilité		
Besoin		**Description**
1	Plus de 72h	Indisponibilité supérieure à 72h acceptée
2	Entre 24h et 72h	Indisponibilité entre 24h et 72h acceptée
3	Entre 4h et 24h	Indisponibilité entre 4h et 24h acceptée
4	Moins de 4h	Indisponibilité inférieure à 4h acceptée

Intégrité		
Besoin		**Description**
1	Non gênant	Pas de besoin d'intégrité
2	Détectable	L'altération doit être identifiée
3	Maîtrisé	L'altération doit être identifiée et corrigée
4	Intègre	Les données doivent être intègres

Confidentialité		
Besoin		**Description**
1	Public	Pas de besoin de confidentialité
2	Réservé	Accessible en lecture par un groupe de personnes ou entités bien identifiées
3	Privé	Accessible en lecture par une seule personne ou entité bien identifiée

Authenticité		
Besoin		**Description**
1	Inconnu	Pas de besoin d'authenticité
2	Identifié	Identité déclarée mais sans garantie d'intégrité
3	Authentique	Identité prouvée

Tableau 3.2 – Critères de sécurité

Niveau		**Description**
1	Négligeable	Pas d'impact constaté
2	Limitée	Impact minime
3	Importante	Impact sérieux mais les dégâts restent réparables
4	Critique	Impact grave, dégâts difficilement ou pas réparables

Tableau 3.3 – Échelle de gravité

Niveau		**Description**
1	Minime	Annuel
2	Significative	Mensuel
3	Maximale	Journalier

Tableau 3.4 – Échelle de vraisemblance

dans le contexte de l'étude. Dans notre cas, les biens essentiels sont les fonctionnalités primaires d'une UAI :

1. **Web** : l'accès de manière générale aux sites Internet et autres services connectés.
2. **Téléphonie** : la ligne téléphonique incluse dans la majorité des offres.
3. **Télévision** : le bouquet de télévision numérique.
4. **NAS** : le stockage de données.

Chaque bien essentiel est matérialisé par la présence de différents biens supports. Ces biens supports sont regroupés en différentes catégories dans EBIOS [3]. Dans cette étude, nous avons retenu des biens supports de 5 types :

1. **Matériels** : alimentation électrique, disque dur.
2. **Organisations** : FAI [4].
3. **Réseaux** : boucle locale, Femto [5], liaison UAI/STB, réseau local, WiFi.
4. **Personnels** : abonné.
5. **Logiciels** : services réseaux WAN [6], services réseaux LAN [7], contrôle parental.

Plusieurs biens supports pouvant servir à différents biens essentiels, le Tableau 3.5 présente la contribution de chaque bien support aux différents biens essentiels.

Biens supports	**Téléphonie**	**NAS**	**Télévision**	**Web**
MAT - Disque dur		✓		
MAT - Alimentation électrique	✓	✓	✓	✓
ORG - FAI	✓		✓	✓
RSX - Réseau local		✓		✓
RSX - WiFi		✓		✓
RSX - Femto	✓			✓
RSX - Liaison UAI / STB			✓	
RSX - Boucle locale	✓		✓	✓
PER - Abonné	✓	✓	✓	✓
LOG - Contrôle Parental				✓
LOG - Services réseaux WAN	✓	✓	✓	✓
LOG - Services réseaux LAN		✓	✓	✓

Tableau 3.5 – Relations entre biens essentiels et biens supports

3. Locaux, systèmes, matériels, logiciels, réseaux, organisations, personnes, papiers, canaux interpersonnels.
4. Fournisseur d'accès à Internet.
5. Mini antenne-relais GSM permettant d'améliorer le signal GSM à domicile.
6. *Wide Area Network* : On regroupe ici tous les logiciels côté WAN : filtrage / firewall, NAT et l'administration de ces services.
7. *Local Area Network* : On regroupe ici tous les logiciels côté LAN : DHCP, DNS et l'administration de ces services.

La dernière étape de l'étude de contexte consiste à identifier les différentes mesures de sécurité existantes. Ces mesures sont utilisées dans le module 5 de la méthode EBIOS et vont permettre de traiter tout ou partie des risques identifiés dans l'étude. Pour les UAI, nous avons identifié 5 mesures de sécurité existantes :

1. **Identification** de l'UAI. Cette identification varie en fonction des opérateurs, elle peut être faite soit par une combinaison d'identifiant/mot de passe, soit par vérification de l'adresse MAC [8] de l'équipement. Cette mesure de sécurité est destinée à empêcher toute personne malveillante d'utiliser illégalement l'infrastructure de l'opérateur afin de bénéficier des services fournis.
2. **Protection physique** offerte par le bâtiment dans lequel se situe l'UAI. Cette mesure permet de protéger l'UAI contre les aléas de la météo (hors phénomènes électromagnétiques) mais aussi contre un accès physique sans autorisation. Ceci permet de réduire le risque d'attaques matérielles directement sur l'UAI.
3. **Authentification WiFi** par clef. Cette mesure permet de s'assurer que seules les personnes en possession de la clef d'authentification peuvent se connecter directement au réseau WiFi.
4. **Cloisonnement WiFi invité**. De nombreuses UAI offrent un second accès WiFi, destiné aux utilisateurs extérieurs ayant un abonnement chez le même fournisseur que celui de l'abonné. Cloisonner cette partie du réseau domestique de l'abonné permet de s'assurer qu'un utilisateur "invité" ne puisse pas accéder au réseau domestique de l'abonné.
5. **Filtrage d'accès**. Chaque UAI est équipée d'un filtre de paquets (pare-feu) empêchant un accès depuis un réseau extérieur à l'UAI.

Ces mesures sont prises en compte dans l'étude, cependant, elles ne modifient pas les événements redoutés, mais elles permettent de limiter la vraisemblance et/ou l'impact d'un événement redouté.

3.1.2 Étude des événements redoutés

L'étude des événements redoutés consiste à déterminer, pour chaque critère de sécurité de chaque bien essentiel, la gravité des impacts, lorsqu'il y a manquement au besoin de sécurité. Différents impacts ont été retenus dans le cadre de l'étude : financier, image de marque, perte de données, juridique, opérationnel, perte de propriété des données. Le besoin de sécurité correspond au niveau attendu de sécurité (ces besoins ont été définis dans le tableau 3.2). Il convient donc de définir pour chaque bien essentiel et pour chaque critère de sécurité :

— le besoin de sécurité attendu,
— les sources de menaces possibles,
— les impacts possibles en cas de manquement au besoin de sécurité,
— la gravité de l'impact.

8. *Media access control* : adresse physique.

	Critères de sécurité			
Biens essentiels	**Disponibilité**	**Intégrité**	**Confidentialité**	**Authenticité**
Web	Important	Négligeable	Critique	Important
NAS	Négligeable	Critique	Négligeable	Négligeable
Téléphonie	Critique	Important	Important	-
Télévision	Limitée	Limitée	Négligeable	Négligeable

Tableau 3.6 – Gravité de l'impact en cas de manquement au besoin de sécurité

Plutôt que de lister ici ces quatre éléments pour chaque bien essentiel et chaque critère de sécurité (ce qui serait fastidieux), nous avons préféré détailler deux exemples ci-dessous et présenter le Tableau 3.6, qui indique la gravité de l'impact en cas de manquement à un besoin de sécurité pour chaque bien essentiel. Il est à noter que nous avons décidé de ne pas retenir le critère d'authenticité pour la téléphonie, dans la mesure où les caractéristiques très particulières de la voix de chacun annulent cet événement redouté. Le contenu de ce tableau doit normalement être établi par le commanditaire de l'étude. Il s'agit donc ici de fournir le point de vue d'un utilisateur de l'UAI. Dans cette étude, nous considérons que le NAS sert uniquement au stockage de données non critiques, ce qui explique qu'un manquement à la confidentialité du NAS est *Négligeable* (nous considérons qu'aucune donnée confidentielle n'est stockée sur le NAS).

Les deux exemples que nous retenons sont :

Web - Confidentialité
Cet événement redouté correspond à la divulgation des données Web échangées entre l'UAI et le FAI.

- Besoin de sécurité : confidentialité réservé (les données que nous envoyons ou recevons sur Internet, à part quelques exceptions comme les données bancaires, peuvent être accessibles à un groupe d'utilisateurs bien définis).
- Sources de menaces [9] : opérateur, personne extérieure malveillante réalisant des attaques réseaux, personne extérieure malveillante réalisant des attaques avec accès physique, utilisateur interne malveillant, virus.
- Impacts : financier (lors d'une transaction bancaire par exemple), image de marque (divulgation d'informations sensibles de l'utilisateur), perte de propriété des données (lors de transfert d'informations confidentielles).
- Gravité : critique (il est très difficile de remédier à la divulgation d'informations).

Téléphone - Disponibilité
Cet événement redouté correspond à la perte de disponibilité du service téléphonique inclus dans l'offre triple-play.

9. L'utilisation d'un protocole sécurisé tel que HTTPS permet de diminuer l'importance de ces menaces mais nous ne pouvons pas considérer que ce protocole soit aujourd'hui systématiquement actif.

— Besoin de sécurité : indisponibilité de moins de 4h (même si les téléphones portables se démocratisent, on a toujours tendance à attacher une certaine confiance à la ligne téléphonique fixe).
— Sources de menaces : opérateur, personne extérieure malveillante réalisant des attaques réseaux, personne extérieure malveillante réalisant des attaques avec accès physique, utilisateur interne malveillant, virus, abonné, problèmes météorologiques (pouvant provoquer des perturbations sur la ligne).
— Impacts : opérationel.
— Gravité : critique (on considère la téléphonie comme un moyen de communication pouvant servir en cas d'urgence).

3.1.3 Étude des scénarios de menaces

L'étude des scénarios de menaces consiste à déterminer la vraisemblance d'occurrence de la défaillance d'un critère de sécurité d'un bien support. Il existe, dans le référentiel EBIOS [10], des types de menaces associés à chaque classe de biens supports. Certains d'entre eux, comme les personnels et les organisations, ont les mêmes types de menaces. Pour les différents types de bien supports identifiés précédemment, nous avons considéré les menaces suivantes :

— **Matériels** : matériel modifié, matériel défaillant, divulgation du contenu, matériel substitué, matériel indisponible.
— **Réseaux** : support dégradé, support substitué, support défaillant, données altérées, données divulguées, données indisponibles.
— **Logiciels** : logiciel indisponible, logiciel supprimé, logiciel modifié, logiciel détourné.
— **Personnel & Organisation** : usurpation d'identité, espionnage, indisponibilité due à une surcharge, atteinte physique, corruption.

Nous définissons ensuite pour chaque bien support et pour chaque critère de sécurité :

1. les sources de menaces envisagées,
2. les menaces existantes,
3. le niveau de vraisemblance d'occurrence de la menace.

Pour cela, au lieu de donner la liste de ces trois éléments pour chaque bien support et chaque critère de sécurité, nous préférons détailler trois exemples. Le Tableau 3.7 indique le niveau de vraisemblance d'occurrence de la menace pour chaque bien support et chaque critère de sécurité [11] de façon synthétique.

Certaines menaces ne sont pas retenues. Il est impossible, par exemple, de traiter la confidentialité ou l'authenticité d'une alimentation électrique. Pour l'abonné, il est difficile d'évaluer la disponibilité ou l'intégrité. Il est important de noter que ce tableau ne reflète en aucun cas le coût de mise en œuvre d'une menace.

10. Ces bases de connaissances sont issues de l'expérience de EBIOS, elles ont pour objectif de guider le rédacteur de l'analyse.
11. Le contenu de ce tableau résulte notamment de l'expertise du personnel expert du CESTI Thales ayant participé à cette étude.

Biens supports	Disponibilité	Intégrité	Confidentialité	Authenticité
Disque dur	Significative	Significative	Significative	-
Alimentation électrique	Minime	Minime	-	-
FAI	Significative	Significative	Minime	Significative
Réseau local	Significative	Minime	Minime	-
WiFi	Significative	Minime	Significative	Minime
Femto	Minime	Minime	Minime	Minime
Liaison UAI / STB	Significative	Minime	Minime	-
Boucle locale	Minime	Minime	Minime	Minime
Abonné	-	-	Minime	Maximale
Contrôle Parentale	Minime	Minime	Minime	-
Services réseaux WAN	Significative	Minime	-	-
Services réseaux LAN	Minime	Minime	-	-

Tableau 3.7 – Niveau de vraisemblance de mise à exécution des menaces

Les trois exemples retenus sont les suivants :

Boucle locale - Confidentialité

Ce scénario de menace correspond à la divulgation des communications échangées sur la boucle locale.

- Sources de menaces : personne extérieure malveillante réalisant des attaques avec accès physique.
- Menaces : divulgation du contenu.
- Vraisemblance : minime.

FAI - Authenticité

Ce scénario de menace correspond à la substitution du FAI de l'abonné.

- Sources de menaces : personne extérieure malveillante réalisant des attaques avec accès physique, personne extérieure malveillante réalisant des attaques réseaux.
- Menaces : usurpation d'identité.
- Vraisemblance : significative.

Services réseaux WAN - Disponibilité

Ce scénario de menace correspond à la perte de disponibilité des services réseau coté WAN de l'UAI.

- Sources de menaces : personne extérieure malveillante réalisant des attaques avec accès physique, personne extérieure malveillante réalisant des attaques réseaux, utilisateur interne malveillant, abonné, virus.
- Menaces : logiciel indisponible, logiciel supprimé.
- Vraisemblance : significative.

3.1.4 Étude des risques

La dernière étape de cette analyse des risques consiste à identifier les différents risques encourus par le système étudié, sachant qu'un risque est la combinaison d'un événement redouté et d'un ou plusieurs scénarios de menaces. Sachant que nous avons défini les différents événements redoutés ainsi que les différents scénarios de menaces, nous pouvons établir la cartographie des risques du système.

Dans EBIOS, il existe deux méthodes pour obtenir les différents risques. La première consiste à établir la liste de tous les scénarios de menaces correspondant à un événement redouté et à considérer que chaque scénario constitue un risque encouru par le système. Dans notre cas cela signifie 81 risques. Pour les obtenir, il suffit de considérer les tableaux 3.5, 3.6 et 3.7. Prenons l'exemple dans le tableau 3.6 de la première case du tableau, correspondant à l'intersection du bien essentiel Web et du critère *disponibilité*. Pour trouver tous les scénarios de menaces pouvant mettre en danger la disponibilité du Web, il suffit d'obtenir la liste des biens supports du Web (qui sont au nombre de 10, comme indiqué dans le tableau 3.5), et de compter ceux pour lesquels des menaces identifiées relatives à l'indisponibilité sont présentes dans le tableau 3.7 (quelle que soit leur vraisemblance). Il y en a 9. En utilisant la même méthode pour toutes les cases du tableau 3.6, on obtient ainsi un total de 81 risques. Cette méthode est à privilégier lorsque l'on souhaite mener une analyse très approfondie.

La deuxième méthode consiste à combiner chaque événement redouté avec tous les scénarios de menaces concernés et ainsi privilégier une représentation "Gravité/-Vraisemblance", qui regroupe tous les événements redoutés selon leur gravité, ainsi que la vraisemblance la plus élevée de tous les scénarios de menaces associés. Pour les obtenir, il suffit, comme pour la première méthode, de considérer les tableaux 3.5, 3.6 et 3.7. Prenons le même exemple, correspondant à l'intersection du bien essentiel Web et du critère *disponibilité* dans le tableau 3.6. La gravité indiquée dans cette case, correspondant à la gravité de cet événement redouté est *Important*. Pour trouver la vraisemblance de cet événement redouté, il faut considérer la vraisemblance la plus élevée de tous les scénarios de menaces dans le tableau 3.7 correspondant aux biens support du Web (qui sont au nombre de 10, comme indiqué dans le tableau 3.5). Parmi les 9 scénarios de menaces correspondants, 5 ont une vraisemblance *Minime* et 4 ont une vraisemblance *Significative*[12]. La vraisemblance la plus élevée est donc *Significative*. L'événement redouté correspondant à l'indisponibilité du Web est donc un risque dont la gravité est *Importante*, et dont la vraisemblance est *Significative*, et se situe donc à l'intersection de la ligne et de la colonne correspondantes, ainsi que présenté dans le tableau 3.8. Dans notre étude, ayant 15 événements redoutés, nous obtenons donc 15 risques, dans ce tableau. Nous optons pour cette seconde méthode, qui a pour avantage de donner une vue plus globale du système étudié.

12. Il faut considérer la vraisemblance de chaque bien support et critère associé ; or la disponibilité du bien support "abonné" n'est pas considérée, ce qui explique pourquoi nous n'avons que 9 scénarios de menaces.

	Vraisemblance		
Gravité	Minime	Significative	Maximale
Négligeable	TV non confidentiel	NAS non accessible NAS non confidentiel Web non intègre	NAS non authentique TV non authentique
Limitée		TV non disponible TV non intègre	
Importante	TEL non confidentiel	TEL non intègre Web non disponible	Web non authentique
Critique		TEL non disponible NAS non intègre Web non confidentiel	

Tableau 3.8 – Analyse des risques

Le Tableau 3.8 représente donc chaque risque en fonction de sa gravité et de sa vraisemblance. Nous avons défini quatre zones de couleur, indiquant le "niveau" de risque. Par la suite nous nous intéressons plus particulièrement à la "zone rouge", contenant les risques dont le niveau de gravité est *Critique* et la vraisemblance *Significative* ou *Maximale*, ainsi que les risques dont le niveau de gravité est *Important* et la vraisemblance est *Maximale*. Cette zone regroupe 4 risques :

— **Téléphonie non disponible**, ce risque est directement lié à la non disponibilité du FAI et des services réseaux coté WAN.
— **NAS non intègre**, ce risque est directement lié à la non intégrité du disque dur. On considère que tant que le disque dur est intègre, les données peuvent être récupérées.
— **Web non confidentiel**, ce risque est principalement dû à la présence d'un point d'accès WiFi. Cependant un second scénario de menaces, encore peu envisagé aujourd'hui, est la possibilité d'écoute sur la boucle locale.
— **Web non authentique**, ce risque exprime la possibilité d'usurpation d'identité du FAI, et par ce fait la faiblesse de l'utilisation de la boucle locale.

En analysant de plus près ces quatre risques, nous constatons que les deux premiers reposent respectivement sur l'efficacité de l'opérateur et la défaillance d'un disque dur. Les deux autres risques de non-respect de la confidentialité et de l'authenticité du Web, expriment chacun des doutes sur la fiabilité de la boucle locale. Ces risques nous ont paru particulièrement intéressants à étudier dans la mesure où aujourd'hui, les scénarios d'attaque connus ne considèrent pas la boucle locale. Ainsi, l'analyse EBIOS que nous avons menée sur les UAI a permis de mettre en avant un scénario d'attaque encore peu exploré. C'est pourquoi la suite de ce cas d'étude s'intéresse à la sécurité du réseau d'accès des fournisseurs d'accès à Internet. Pour cela nous avons, dans un premier temps, mené une étude comparative des séquences de démarrage, d'un point de vue réseau, de différentes UAI distribuées en France. Ensuite, nous avons exploré ces faiblesses en effectuant tout d'abord une simulation du fournisseur de service sur la boucle locale puis en effectuant des attaques.

3.2 Etude comparative des UAI

Dans cette section, nous nous intéressons à la boucle locale et à la place qu'elle occupe dans la sécurité des réseaux informatiques domestiques. Afin de tester les éventuelles faiblesses des UAI vis-à-vis de cette boucle locale, nous avons conçu une plateforme d'observation de boucle locale ADSL, afin d'observer les échanges réalisés sur ce tronçon du réseau entre le FAI et l'abonné. Pour cette étude, nous avons eu à notre disposition six UAI représentant une grande majorité des UAI déployées en France au moment de l'étude. Pour chacune d'entre elles, nous avons déployé notre méthode d'écoute et observé les données échangées avec le FAI lors de la phase de démarrage de l'UAI.

Dans un premier temps nous discutons les différents types de supports physiques utilisés pour les boucles locales, et plus particulièrement, le fonctionnement de la paire de cuivre. Ensuite, dans un second temps, nous présentons notre plateforme d'observation de boucle locale ADSL. Finalement, nous discutons les résultats de de l'étude comparative que nous avons menée sur notre panel d'UAI.

3.2.1 La boucle locale

Il existe globalement quatre types de supports physiques utilisés comme boucle locale : la paire de cuivre, le câble, les fibres optiques et les ondes radio. Dans la suite, nous nous intéressons uniquement à la paire de cuivre, historiquement installée par l'opérateur téléphonique, et qui reste aujourd'hui le support le plus utilisé en France. En effet, au quatrième trimestre 2014, l'ARCEP [13] [12] affirme que 86% des connexions, à l'Internet haut et très haut débit, se font en utilisant la paire de cuivre (technologies xDSL). Il est important de noter que nos expériences sont compatibles avec les autres types de boucles locales en utilisant du matériel analogue.

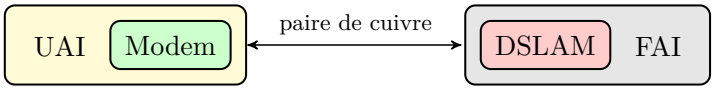


Figure 3.1 – La boucle locale

La paire de cuivre est reliée côté abonné à un MoDem et à un DSLAM [14] côté opérateur (cf. Figure 3.1). Ces deux équipements modulent et démodulent un signal analogique, transmis sur la paire de cuivre à haute fréquence, en signaux numériques (et inversement).

13. Autorité de régulation des communications électroniques et des postes
14. *Digital subscriber line access multiplexer*

3.2.2 Plateforme d'écoute sur une boucle locale

Afin de capturer toutes les communications ADSL circulant sur une paire de cuivre, plusieurs méthodes existent :

— Par **écoute** : dupliquer le signal analogique et le démoduler sans connaître aucun des paramètres utilisés lors de la négociation ADSL ;

— Par **attaque de l'homme du milieu** : démoduler et remoduler le signal en s'interposant dans la négociation ADSL.

La première solution nécessite des connaissances avancées en traitement du signal. Pour la mise en œuvre de cette solution, il est indispensable de développer un outil capable de se synchroniser passivement sur une connexion entre un DSLAM et un MoDem. Non seulement la présence de ce dispositif peut perturber voire empêcher la transmission des données entre le MoDem et le DSLAM (phénomène d'écho), mais ces problèmes spécifiques se situent hors du cadre des travaux de cette thèse. En revanche, la seconde solution peut être réalisée à l'aide d'équipements accessibles au grand public. Nous avons donc adopté cette seconde méthode pour notre plateforme [18].

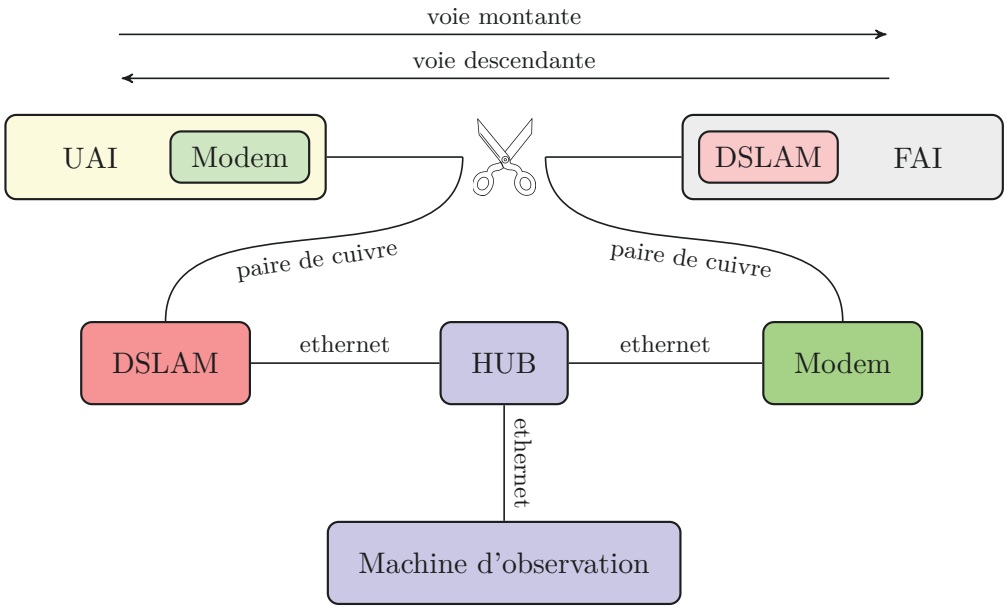


FIGURE 3.2 – Plateforme d'observation d'une boucle locale ADSL

Le DSLAM et le MoDem transmettent sur des bandes de fréquences différentes. Autrement dit, la modulation utilisée sur la voie montante (MoDem vers DSLAM) diffère de celle utilisée sur la voie descendante (DSLAM vers MoDem). Inversement, le MoDem doit être capable de démoduler sur la voie descendante tandis que le DSLAM doit être capable de démoduler sur la voie montante (cf. Figure 3.2). Par conséquent, il est possible de couper physiquement la ligne téléphonique et d'y insérer un DSLAM et un MoDem supplémentaires, tout en assurant la connectivité

entre l'opérateur et l'abonné.

En réalité, cette modification change la manière dont l'UAI communique avec l'opérateur : elle se synchronise et communique avec le nouveau DSLAM ; le nouveau DSLAM communique avec le nouveau MoDem qui, à son tour, se synchronise et communique avec le DSLAM de l'opérateur. Étant donné que l'interface vers le réseau local de la plupart des MoDem et DSLAM est de type Ethernet, cette plateforme revient donc à transformer un tronçon de cuivre en deux tronçons de cuivre distincts interconnectés par un réseau Ethernet (cf. Figure 3.2). Comme l'écoute sur un réseau Ethernet est très facile, les communications envoyées et reçues par l'UAI peuvent être étudiées.

Cette configuration nous a permis de procéder à une étude comparative des différents protocoles mis en œuvre lors de la phase de démarrage de différentes UAI déployées en France [16]. La suite de cette section présente les résultats de cette étude.

3.2.3 Résulats de l'étude comparative

Globalement, tous les opérateurs utilisent PPP, IPv4, et des protocoles UDP et TCP standards, tels que DNS, SIP, NTP et HTTP. Certains opérateurs utilisent également des protocoles chiffrés à base de SSL [15].

Nous avons constaté que chaque requête auprès d'un serveur spécifique est précédée d'une requête DNS afin d'obtenir l'adresse IP correspondant à l'URL du serveur. Ce comportement s'avère systématique, même si le serveur a déjà été contacté précédemment. Ceci nous a permis de déduire de nombreuses informations sur les services utilisés et plus généralement, sur la séquence de démarrage. Cette séquence de démarrage est relativement similaire, quelle que soit l'UAI étudiée, et se compose de quatre étapes (détaillées par la suite) : 1) ATM [16], 2) PPP, 3) Configuration et 4) SIP.

Les résultats de cette étude sont rassemblés dans le Tableau 3.9. La première colonne contient l'identifiant de l'UAI (de manière anonyme). La deuxième colonne contient les principaux paramètres utilisés pour la négociation ATM. La troisième colonne indique si l'opérateur utilise PPP, et si tel est le cas, quel protocole d'authentification est utilisé. La quatrième colonne indique si l'opérateur utilise le protocole DHCP afin d'attribuer une adresse IP à l'UAI. La cinquième colonne indique l'algorithme de hachage utilisé lors de l'enregistrement auprès du serveur SIP. Finalement, les deux dernières colonnes montrent les protocoles utilisés lors des phases de configuration et de mise à jour.

15. PPP : Protocole Point à Point, UDP : User Datagram Protocol, TCP : Transmission Control Protocol, DNS : Domain Name System, SIP : Session Initiation Protocol, NTP : Network Time Protocol, HTTP : HyperText Transfer Protocol, SSL : Secure Sockets Layer.

16. *Asynchronous Transfer Mode*, protocole de niveau 2 permettant un multiplexage à répartition dans le temps de différents flots de données.

UAI	ATM	PPP	DHCP	SIP	Configuration	Mise à jour
A	8/35/LLC	chap	non	MD5	HTTP, FTP, SSL	-
B	8/35/LLC	chap	oui	MD5	HTTP, SSL	SSL
C	8/36/VC	non	oui	MD5	SSL	-
D	8/35/LLC	chap	oui	MD5	HTTP	HTTP
E	8/35/LLC	chap	oui	MD5	HTTP	HTTP
F	8/35/LLC	chap	non	MD5	SSL	-

Tableau 3.9 – Caractéristiques de plusieurs UAI ADSL déployées en France

3.2.3.1 ATM

La plupart des fournisseurs utilisent des paramètres similaires pour le protocole ATM. Ces paramètres sont très souvent communiqués ouvertement par le fournisseur permettant à l'utilisateur d'utiliser son propre MoDem, configuré manuellement, à la place de l'UAI fournie par l'opérateur. À l'issue de nos observations, seules quatre combinaisons de paramètres apparaissent. Tant que l'opérateur utilise des paramètres relativement standards, l'écoute d'une communication ADSL reste relativement simple. Dans le cas contraire, ces paramètres peuvent être obtenus grâce à des techniques de rétro-ingénierie.

3.2.3.2 PPP

Ce protocole est fréquemment utilisé lorsque les opérateurs doivent partager la boucle locale [98] avec l'opérateur téléphonique historique. Nous avons noté à ce jour un seul opérateur qui a totalement abandonné ce protocole. D'autres fournisseurs implémentent le protocole mais sur une interface virtuelle séparée. La plupart du temps, cette interface n'est pas utilisée pour le transfert de données. Ceci permet à l'opérateur de réduire les surcharges lors de la transmission de données tout en conservant la compatibilité dans les situations où PPP est encore requis.

3.2.3.3 SIP

SIP est le protocole le plus fréquemment utilisé pour la téléphonie sur IP, et donc sur Internet. Un client SIP, qui dans notre cas est inclus dans l'UAI, utilise un nom d'utilisateur et un mot de passe afin de se connecter au serveur SIP. Il existe différentes procédures permettant de sécuriser l'établissement d'une session SIP (HTTP Basic, S/MIME, HTTP Digest, TLS ou IPSec). En observant les négociations plus en détail, nous avons constaté que tous les opérateurs utilisent le même protocole, HTTP Digest, tel que présenté dans la Figure 3.3 :

— Une demande d'enregistrement vide est envoyée par le client SIP ;
— Cette requête est refusée par le serveur, qui renvoie un message "Authentication Required", incluant un "*nonce*" ;
— Le client SIP s'enregistre ensuite auprès du serveur SIP en fournissant une

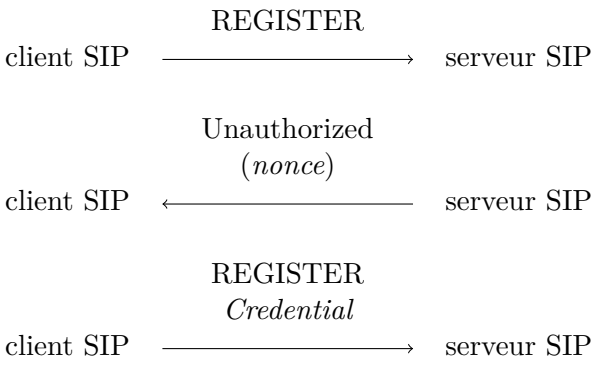


FIGURE 3.3 – Enregistrement SIP - HTTP Digest

empreinte MD5 [17] calculée principalement à partir du *nonce* et du mot de passe SIP (que le client SIP connaît ou est capable de calculer).

Bien que l'utilisation de l'algorithme de hachage MD5 soit déconseillée depuis plusieurs années déjà, à cause de certaines vulnérabilités prouvées [99], toutes les UAI utilisent MD5 pour générer l'*empreinte* de leurs réponses.

Cependant, en considérant que 1) le *nonce* varie régulièrement et aléatoirement [90], 2) le mot de passe est suffisamment long pour résister aux attaques en force brute et 3) le mot de passe est suffisamment imprévisible pour être considéré comme quasi aléatoire, alors une empreinte MD5 peut être considérée suffisamment sûre.

3.2.3.4 Configuration

Les UAI sont conçues pour permettre à l'utilisateur de profiter pleinement de tous les services fournis tels que la télévision et la téléphonie. Afin de permettre à ces services de fonctionner correctement, une configuration spécifique est nécessaire. Cette configuration est obtenu par les UAI via des échanges avec les serveurs du FAI.

La configuration d'une UAI est donc une phase très importante de la procédure de démarrage. De ce fait, dans la plupart des cas, cette phase utilise des méthodes cryptographiques, soit pour authentifier l'UAI auprès du fournisseur, soit pour protéger le contenu des échanges. Sans connaissance particulière de l'infrastructure de l'opérateur, il devient donc très difficile d'identifier et de caractériser ces connexions. Cependant, comme annoncé dans l'introduction de cette section, avant d'accéder à un serveur, une requête DNS est envoyée afin d'obtenir l'adresse IP du serveur. Il s'avère que la requête DNS révèle d'importantes informations concernant l'échange. Par exemple, si le nom de domaine du serveur contacté contient le terme TR69 [18] ou un équivalent, il est raisonnable de supposer que ces échanges concernent la phase

17. *Message Digest 5.*
18. TR69 ou CWMP : *CPE WAN Management Protocol.*

de configuration.

Les protocoles utilisés pour transmettre la configuration, sont présentés dans l'avant-dernière colonne du Tableau 3.9. Nous constatons que les différents opérateurs n'utilisent pas tous les mêmes protocoles pour envoyer à l'UAI sa configuration. La plupart des fournisseurs utilisent le protocole sécurisé HTTPS [19]. Pour les UAI A et B, l'échange SSL est précédé par un échange utilisant le protocole non sécurisé HTTP afin de déclarer la présence de l'équipement sur le réseau. En observant de plus près l'implémentation du protocole SSL chez les différents opérateurs, nous avons constaté l'utilisation de deux algorithmes d'échanges, **TLS_RSA_WITH-_RC4_128_SHA** et **TLS_RSA_WITH_AES_256_CBC_SHA**. Tous deux sont conformes aux recommandations émises par l'ANSSI [71]. Cependant, lorsque nous nous intéressons aux UAI D et E, nous pouvons voir que seul le protocole non sécurisé HTTP est utilisé. Cette faille de sécurité nous permet, pour ces deux UAI, d'observer la configuration lors de leur démarrage. De plus, les données échangées ne sont pas signées, ce qui rend cette faille exploitable. L'utilisation d'une signature nous permettrait uniquement de lire l'échange, et non de le modifier.

3.2.3.5 Mise à jour

Plusieurs UAI permettent à l'utilisateur final de vérifier la présence d'un nouveau firmware manuellement, et dans ce cas, de déclencher la mise à jour. D'autres UAI vérifient la présence d'un nouveau firmware automatiquement lors du démarrage de l'UAI. Nous avons analysé différents échanges initiés lors de ce processus. Les résultats montrent que les protocoles utilisés, lors d'une mise à jour, sont les mêmes que ceux employés lors de la phase de configuration. Ceci implique que la phase de mise à jour des UAI D et E n'est pas sûre. Comme lors de la phase de configuration, nous sommes capables d'observer et/ou de modifier le contenu du firmware lors de cette procédure.

3.2.3.6 Observations

Pour résumer ces expérimentations, globalement, les principales UAI françaises fonctionnent de la même manière. Cependant, certaines UAI diffèrent significativement des autres sur un point : la protection des phases de configuration et de mise à jour. Dans la suite de ce chapitre, nous nous intéressons aux conséquences des faiblesses présentes dans les protocoles mis en œuvre entre l'opérateur et l'UAI.

3.3 Exploration des faiblesses

Afin d'analyser plus en détail les protocoles mis en œuvre entre l'opérateur et l'UAI, nous avons simulé le comportement du service de mise à jour du fournisseur d'accès à Internet. Ces simulations ont été réalisées grâce à une plateforme de simu-

19. *Secure HTTP*

lation d'un fournisseur de services sur Internet, que nous avons construite à partir de notre plateforme d'observation.

Nous présentons d'abord notre plateforme de simulation avant de montrer comment nous l'avons utilisée pour simuler tout d'abord un FAI légitime puis pour mener des attaques.

3.3.1 Simulation d'un fournisseur de services sur Internet

Cette plateforme (cf. Figure 3.4) est destinée à simuler les services fournis sur la boucle locale par le fournisseur d'accès à Internet (FAI). La mise en œuvre de cette plateforme est fondée sur les connaissances acquises en observant la boucle locale utilisant la plateforme d'écoute. Ici, au lieu de relier notre DSLAM au réseau de l'opérateur grâce à un MoDem, nous l'avons relié à un ordinateur capable de simuler le comportement du fournisseur de services. Nous avons installé et configuré les différents éléments au fur et à mesure, en suivant notre méthode itérative, décrite dans la section 2.2.2. Pour rappel, cette méthode est fondée sur l'observation des requêtes émises par l'UAI et la fabrication de réponses associées, de façon itérative, simulant ainsi le ou les service(s) qui en principe communique(nt) avec l'UAI sur ce lien.

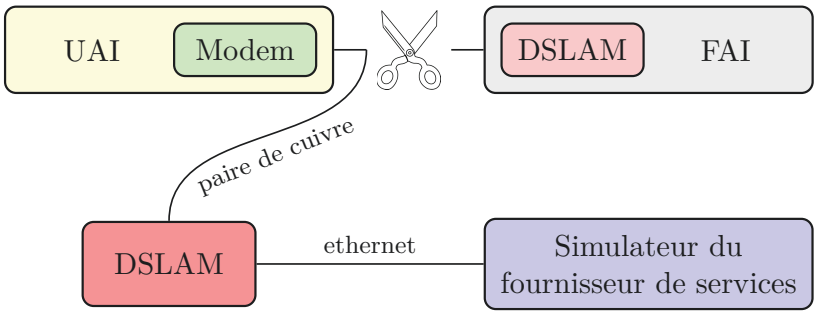


Figure 3.4 – Simulation d'un fournisseur de services sur Internet

Nous savons qu'une multitude de services sont nécessaires au bon fonctionnement d'une UAI chez l'abonné. Cependant, lors de notre étude, nous nous sommes rendus compte, en déroulant la méthode itérative, que tous ces services ne sont pas nécessairement actifs lorsque l'UAI annonce à son possesseur être opérationelle. Les deux principaux services permettant d'atteindre cet état chez la majorité des UAI sont les suivants :

— **PPP** : au démarrage, pour les opérateurs utilisant PPP, les UAI cherchent d'abord à s'authentifier auprès de l'opérateur selon le protocole PPP.
— **DNS** : des équipements embarqués, tels que les UAI, connaissent rarement les adresses IP des serveurs avec lesquels elles doivent communiquer. Il est donc nécessaire de déployer un serveur DNS afin de permettre à l'UAI d'initier ses requêtes.

Finalement, pour simuler correctement le service de mise à jour, nous avons dû installer un service HTTP. Nous avons représenté le déroulement complet de cette démarche dans la Figure 3.5.

3.3.2 Conduite d'attaque

Nous avons plus particulièrement analysé la procédure de mise à jour. Lorsque la mise à jour utilise le protocole sécurisé HTTPS, il n'est pas possible d'imiter le serveur de l'opérateur, car nous ne sommes pas en possession des certificats utilisés. Par conséquent, l'UAI refuse systématiquement de communiquer avec notre plateforme. Ce problème ne se pose pas avec le protocole non sécurisé HTTP.

La majorité des UAI observées lors de nos expériences utilisent un firmware propre au fabricant (cf. section 1.2.3). Cependant, les UAI D et E utilisent un firmware générique, pour lequel les procédures ainsi que les outils de génération et de modification sont publiquement disponibles. C'est pourquoi, tout en nous inspirant des informations obtenues lors de la phase d'observation, nous sommes parvenus à créer notre propre firmware et à l'installer au sein de l'UAI. Ce firmware est identique à celui fourni par l'opérateur aux détails près suivants :

— Nous avons désactivé le pare-feu. Ceci autorise l'accès au service SSH depuis l'interface WAN ;
— Nous avons désactivé la procédure de mise à jour ;
— Nous avons installé un logiciel permettant d'initier à distance des appels téléphoniques potentiellement surtaxés depuis l'abonnement associé à l'UAI.

Ces trois modifications permettent de contrôler entièrement l'UAI à distance. Il n'y a aucune différence de fonctionnement pour l'utilisateur. En effet, tous les services (Internet, téléphone et télévision) continuent de fonctionner normalement. L'impact direct pour l'utilisateur se verra sur sa facture à la fin du mois lorsque les appels sur-taxés seront facturés.

3.4 Compétences et vraisemblance : discussion

Les compétences techniques requises pour mettre en œuvre une attaque comme celle décrite dans ce chapitre ne sont pas l'unique enjeu. En effet, d'autres caractéristiques de l'attaquant, comme les moyens financiers dont il dispose ou le temps qu'il est prêt à y consacrer, sont à considérer. De ce fait, il est important de considérer ces aspects afin de pouvoir évaluer correctement la vraisemblance de ce scénario de menaces. Dans le cadre de cette étude, nous considérons particulièrement les `compétences techniques`, les `moyens financiers`, le `temps`, l'`autorité` [20] et le `renseignement` [21].

20. Capacité à convaincre un individu à réaliser un acte contre son intérêt. Cette autorité peut être acquise de par la fonction (i.e. : policier, pompier, etc.) de l'attaquant, ou la fonction qu'il imite (i.e. : l'attaquant se fait passer pour le helpdesk de l'opérateur).

21. Accès aux bases de données de renseignements des différents organismes d'État et autres instances contenant des informations personnelles sur l'individu ciblé.

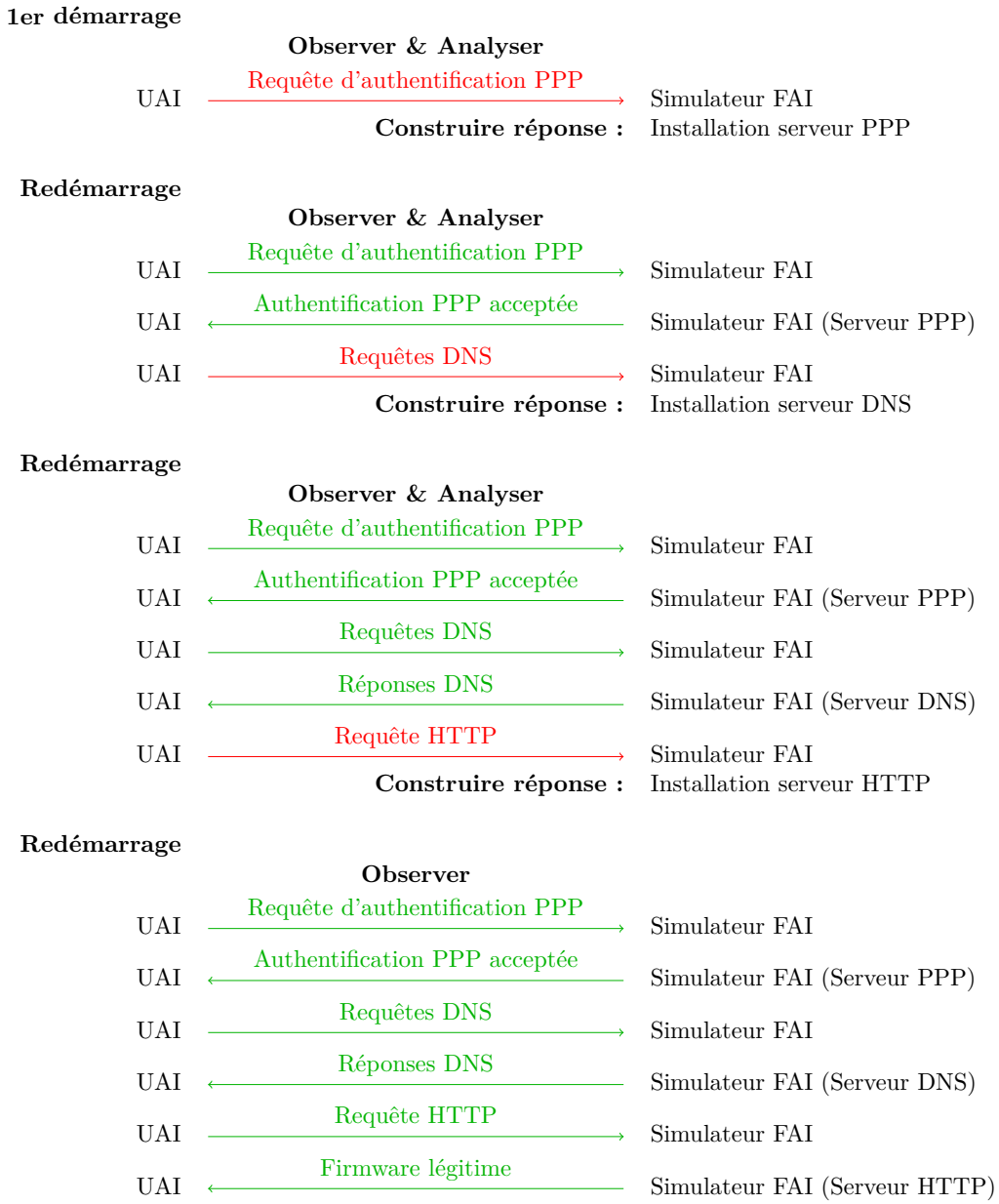


FIGURE 3.5 – Séquence de démarrage et de mise à jour du firmware

Lors de l'appréciation des risques, dans la première partie de ce chapitre, nous n'avons pas distingué les sources de menaces selon leur niveau de compétence. La seule source de menace ciblant la confidentialité ou l'intégrité de la boucle locale est une `personne extérieure malveillante réalisant des attaques avec accès physique`. Or, cette source peut être incarnée par différents profils ayant des niveaux de compétence différents. Par exemple, un officier de police n'aura pas la même autorité ni les mêmes moyens financiers qu'un mouvement activiste. Dans le Tableau 3.10, nous avons décrit 3 profils différents avec leurs caractéristiques respectives.

Profil	**Caractéristiques**				
	Compétences techniques	Moyens financiers	Temps	Autorité	Renseignement
Entité étatique	Important	Important	Important	Important	Important
Groupe activiste	Important	Moyen	Important	Faible	Moyen
Script kiddie	Important	Faible	Moyen	Néant	Faible

Tableau 3.10 – Caractéristiques des profils d'attaquant.

Sans être exhaustif, ce tableau permet d'illustrer la différence entre les différents profils d'attaquant. Suite aux expériences discutées dans ce chapitre, nous sommes capables de définir les différentes caractéristiques requises pour mener à bien ces attaques. Nous avons repris ces caractéristiques dans le Tableau 3.11.

Caractéristique	Compétences techniques	Moyens financiers	Temps	Autorité	Renseignement
Niveau	Moyen	Moyen	Faible	Important	Moyen

Tableau 3.11 – Compétences requises.

Ceci nous permet de constater, a priori, qu'un *script kiddie* possède les compétences techniques et le temps suffisant pour mener à bien les attaques décrites dans ce chapitre. Cependant, il ne possède probablement ni les moyens financiers, ni l'autorité, ni les renseignements requis. Ainsi, même si ces attaques restent relativement simples à mettre en œuvre, les autres conditions nécessaires les rendent assez peu probables, même si leurs effets peuvent être critiques, comme nous l'avons montré dans ce chapitre. En revanche, du point de vue de tous les critères considérés, ces attaques sont tout à fait à la portée d'une organisation ayant des moyens et des ambitions.

3.5 Conclusion

Dans ce chapitre, nous avons mis en évidence l'existence de certaines failles de sécurité dans la conception des réseaux d'accès des fournisseurs d'accès à Internet. Le déroulement pas à pas de notre méthode d'analyse nous a permis d'aboutir à ce

résultat. Dans un premier temps, nous nous sommes servis de la méthode EBIOS afin d'apprécier les différents risques liés aux UAI. Cette étape clef nous a permis de mettre en évidence les différents risques relatifs à cet équipement. La rigueur de cette méthode nous a également conduit a déceler plusieurs scénarios de menaces relatifs à chaque risque.

Dans le cadre de cette étude, nous avons décidé d'en étudier un en particulier, le réseau d'accès. Ensuite, la deuxième étape de notre méthode a permis de valider d'un point de vue technique la possibilité d'exploiter ce scénario. Pour cela, nous avons mis en œuvre une plateforme spécifique permettant d'observer la boucle locale ainsi qu'une deuxième plateforme permettant de simuler le service de mise à jour du FAI.

L'UAI est par définition une passerelle entre le réseau Internet et le réseau informatique domestique. Ceci signifie que d'autres communications, provenant d'autres équipements grand public connectés à Internet, transitent à travers l'UAI et la boucle locale. Ainsi, il est donc possible d'analyser les communications entre ces équipements connectés et leurs fournisseurs de contenu respectifs à l'aide des plateformes décrites dans ce chapitre. Par exemple, les téléviseurs connectés reçoivent, pour la plupart, leur mise à jour via Internet. Les communications entre le téléviseur et le service de mise à jour du fabricant sont donc observables et peuvent être simulées grâce à ces plateformes. Notre second cas d'étude, présenté dans le chapitre suivant, est justement consacré à l'étude de la sécurité des téléviseurs connectés à Internet et ses réseaux d'accès, et ce point sera, entre autres, abordé.

Nous avons également constaté que l'utilisation de protocoles sécurisés, tels que HTTPS, permet d'éviter l'observation et la simulation des communications sur ce tronçon. L'utilisation de tels protocoles constitue en effet la première contre-mesure face au scénario de menace étudié. Nous pensons cependant que d'autres contre-mesures, parfois simples, existent. Nous aborderons cet aspect dans le dernier chapitre de cette thèse.

Chapitre 4

Cas d'étude 2 : Téléviseur connecté & réseaux d'accès

Sommaire

Ce chapitre présente le second cas d'étude de cette thèse, à savoir l'étude des téléviseurs connectés à Internet, également connus sous le nom de Smart-TV, et de leurs réseaux d'accès. Comme pour les UAI, nous commençons ce cas d'étude en appliquant la méthode EBIOS. Nous verrons comment cette analyse nous a orientés

vers l'étude des flux TV hertziens ainsi que l'analyse des données échangées avec des services distants sur Internet. Le réseau hertzien est unidirectionnel, ce qui signifie que son contenu est identique pour tous ceux qui le reçoivent. À notre connaissance, peu d'études concernant sa sécurité lui sont consacrées. Aujourd'hui, ce réseau permet de transmettre du contenu interactif vers le téléviseur afin d'exploiter ensuite la connexion Internet. Ceci implique que des données à caractère privé peuvent être envoyées sur Internet à l'insu de l'utilisateur. De plus, ce contenu interactif peut potentiellement contenir du code malveillant, permettant de compromettre le réseau informatique du domicile. En considérant tout ceci, il devient légitime de considérer la sécurité des téléviseurs connectés et de ses réseaux d'accès. La deuxième partie de ce chapitre présente les expériences techniques mises en œuvre afin de mettre en évidence certaines failles de sécurité et des cas de non respect de la vie privée.

4.1 Analyse des risques d'un téléviseur connecté

Dans cette première phase de notre cas d'étude concernant les téléviseurs connectés, nous allons suivre la méthode EBIOS décrite dans la section 2.1.2.5. Nous présentons comment cette analyse nous a permis d'identifier un scénario de menace original encore peu exploré. La suite de ce chapitre présente les expérimentations menées visant à valider ce risque, ainsi que certains scénarios de menaces soulevés par l'étude.

Dans le chapitre précédent, notre premier cas d'étude a permis d'illustrer en détail chaque étape de l'étude. Ici, nous ne rappelons que brièvement chaque étape en privilégiant les explications lorsque nous avons fait des choix différents de ceux de l'étude précédente.

4.1.1 Contexte de l'étude

4.1.1.1 Objectifs et cadre de l'étude

Le but de cette analyse est d'identifier les risques associés à l'utilisation des téléviseurs connectés à Internet, et de les prioriser par ordre d'importance du point de vue des habitants du domicile, appelés "téléspectateurs" par la suite. Pour cette étude, nous considérons une utilisation privée du téléviseur, et nous réalisons cette étude du point de vue du téléspectateur. Dans le contexte des téléviseurs connectés, nous avons identifié les 9 sources de menaces présentées dans le Tableau 4.1.

4.1.1.2 Définition des métriques

Nous retenons ici les mêmes critères, avec leur échelles respectives, que ceux utilisés lors du premier cas d'étude : *disponibilité, intégrité, confidentialité* et *authenticité*. Nous considérons qu'une modification des données par interposition d'un équipement malveillant sur un lien de communication est un défaut d'*authenticité*, car l'émetteur n'est plus l'émetteur légitime. Un défaut d'*intégrité* doit être occasionné sans coupure physique du lien entre les deux entités de la communication,

Sources de menaces	Humain	Int/Ext	Malveillant
Utilisateur interne malveillant	✓	Int	✓
Utilisateur interne maladroit	✓	Int	
Personne extérieure malveillante à proximité du domicile	✓	Ext	✓
Personne extérieure malveillante	✓	Ext	✓
Opérateur TV	✓	Ext	
Opérateur VoD	✓	Ext	
Fabricant TV	✓	Ext	
Virus[1]		Ext	✓
Problèmes météorologiques		Ext	

1. Représente tout type de maliciel se propageant de façon autonome.

Tableau 4.1 – Sources de menaces

comme un phénomène naturel ou un brouilleur malveillant par exemple. Les échelles utilisées pour la gravité et la vraisemblance sont également identiques à celles utilisées lors du premier cas d'étude (cf. Section 3.1.1.2).

4.1.1.3 Identification des biens

Dans le cadre de cette étude, nous distinguons les biens essentiels suivants pour un téléviseur connecté :

1. **TV (temps réel)** : service permettant de regarder des émissions télévisées en temps réel.
2. **VoD** [2] : service permettant de commander et de regarder des vidéos à la demande.
3. **PVR** [3] : service permettant d'enregistrer une émission télévisée en temps réel sur un support de stockage physique, comme un disque dur par exemple.
4. **TV Interactive** : service permettant d'accéder au contenu interactif des chaînes TV.
5. **Lecteur Multimédia Réseau (LMR)** : service permettant de lire du contenu multimédia à travers le réseau informatique du domicile.

Chaque bien essentiel est matérialisé par la présence de différents biens supports. Dans cette étude, nous avons identifié des biens supports de trois types :

1. **Organisations** *(ORG)* : opérateur TV, fournisseur du contenu VoD.
2. **Réseaux** *(RSX)* : accès à Internet, réseau local, canal TV.
3. **Logiciels** *(LOG)* : système d'exploitation.

Le Tableau 4.2 présente la contribution de chaque bien support aux différents biens essentiels du système.

2. Video on Demand
3. Personal Video Recorder

Biens supports	TV (temps réel)	VoD	PVR	TV interactive	LMR
RSX - Accès Internet		✓		✓	
RSX - Réseau local		✓		✓	✓
RSX - Canal TV	✓		✓	✓	
LOG - Système d'exploitation	✓	✓	✓	✓	✓
ORG - Opérateur TV	✓		✓	✓	
ORG - Fournisseur contenu VoD		✓			

Tableau 4.2 – Relations entre biens essentiels et biens supports

	Critères de sécurité			
Biens essentiels	**Disponibilité**	**Intégrité**	**Confidentialité**	**Authenticité**
TV (temps réel)	Critique	Limitée	Importante	Importante
VoD	Limitée	Limitée	Importante	Limitée
PVR	Négligeable	Limitée	Importante	Limitée
TV interactive	Négligeable	Limitée	Importante	Critique
Lecteur Multimédia Réseau	Négligeable	Limitée	Importante	Importante

Tableau 4.3 – Gravité de l'impact en cas de manquement au besoin de sécurité

4.1.2 Étude des événements redoutés

Nous rappelons que l'étude des événements redoutés consiste à déterminer, pour chaque critère de sécurité de chaque bien essentiel, la gravité des impacts, lorsqu'il y a manquement au besoin de sécurité. Il convient donc de définir pour chaque bien essentiel et pour chaque critère de sécurité :

— le besoin de sécurité attendu,
— les sources de menaces possibles,
— les impacts possibles en cas de manquement au besoin de sécurité,
— la gravité de l'impact.

Différents impacts ont été retenus dans le cadre de l'étude : absence d'activité, absence d'information (ou informations erronées), perte de données privées [4], perte financière, divulgation d'activité.

Comme lors du chapitre précédent, plutôt que de lister ici ces quatre éléments pour chaque bien essentiel et chaque critère de sécurité, nous avons préféré détailler deux exemples ci-dessous et présenter le Tableau 4.3, qui indique la gravité de l'impact en cas de manquement à un besoin de sécurité pour chaque bien essentiel.

Nous détaillons ci-dessous les deux événements redoutés que nous aborderons plus en détail lors de la deuxième partie de ce chapitre.

Télévision (temps réel) - Confidentialité
Cet événement redouté correspond à la divulgation de l'activité du téléspectateur,

4. On considère ici les enregistrements réalisés à l'aide du PVR ainsi que toute autre donnée privée stockée sur l'espace de stockage dédié au téléviseur.

Biens supports	Disponibilité	Intégrité	Confidentialité	Authenticité
Accès Internet	Significative	Minime	Minime	Significative
Réseau local	Minime	Minime	Minime	Minime
Canal TV	Minime	Maximale	-	Significative
Système d'exploitation	Minime	Minime	Significative	Significative
Opérateur TV	Minime	Minime	Significative	Significative
Fournisseur contenu VoD	Significative	Minime	Significative	Significative

Tableau 4.4 – Niveau de vraisemblance de mise à exécution des menaces

i.e., divulgation des chaînes regardées.

- Besoin de sécurité : réservé (l'information indiquant la chaîne TV que l'utilisateur regarde peut être connue de tous les acteurs permettant au téléspectateur de regarder une émission télévisée : la chaîne TV en tant qu'organisation, l'opérateur du canal TV et le téléspectateur).
- Sources de menaces : personne malveillante à proximité du domicile, virus.
- Impacts : divulgation d'activité.
- Gravité : importante (on considère que de plus en plus d'individus sont préoccupés par le respect de leur vie privée).

TV interactive - Authenticité

Cet événement redouté correspond à l'altération des données informatiques incluses dans l'émission télévisuelle, permettant en temps normal de fournir un service interactif au téléspectateur.

- Besoin de sécurité : authentique (la TV interactive nécessite l'exécution de code sur le téléviseur, celui-ci ne doit pas affecter la sécurité de ce dernier).
- Sources de menaces : personne malveillante à proximité du domicile, opérateur TV, virus.
- Impacts : absence d'information.
- Gravité : critique (la TV interactive nécessite l'exécution de code informatique sur le téléviseur, c'est pourquoi il est primordial de connaître la source du contenu).

4.1.3 Étude des scénarios de menaces

L'étude des scénarios de menaces consiste à déterminer la vraisemblance d'occurrence d'une menace pour chaque critère de sécurité de chaque bien support. Pour cela, nous définissons pour chaque bien support et pour chaque critère de sécurité :

1. les sources de menaces envisagées,
2. les menaces existantes,
3. le niveau de vraisemblance de mise à exécution de la menace.

Ici également, au lieu de donner la liste de ces trois éléments pour chaque bien support et chaque critère de sécurité, nous préférons détailler trois exemples également présentés dans le Tableau 4.4, qui indique le niveau de vraisemblance de mise à exécution de la menace pour chaque bien support et chaque critère de sécurité. Nous n'avons pas retenu la confidentialité du canal TV, car nous considérons que ce scénario de menace n'a pas de sens. En effet, une émission télévisuelle classique gratuite, est diffusée sans restriction d'accès et est identique pour tout le monde. Les trois exemples retenus sont ceux abordés dans la deuxième partie de ce chapitre.

Canal TV - Authenticité
Ce scénario de menace correspond à la substitution du canal télévisuel utilisé par le téléviseur afin de recevoir le contenu des chaînes TV.

— Sources de menaces : personne malveillante à proximité du domicile.
— Menaces : données altérées.
— Vraisemblance : Significative.

Accès Internet - Authenticité
Ce scénario de menace correspond à la substitution du canal Internet utilisé par le téléviseur afin d'accéder aux services interactifs sur Internet.

— Sources de menaces : personne malveillante à proximité du domicile.
— Menaces : données altérées, support substitué.
— Vraisemblance : Significative.

Accès Internet - Confidentialité
Ce scénario de menace correspond à la divulgation des données émises et reçues par le téléviseur sur Internet.

— Sources de menaces : personne malveillante à proximité du domicile, virus.
— Menaces : données divulguées.
— Vraisemblance : Minime.

4.1.4 Étude des risques

La dernière étape de notre analyse des risques consiste à identifier les différents risques encourus par le système étudié, sachant qu'un risque est la combinaison d'un événement redouté et d'un ou plusieurs scénarios de menaces. Maintenant que nous avons défini les différents événements redoutés ainsi que les différents scénarios de menaces, nous pouvons établir la cartographie des risques du système.

Ici également, nous privilégions une représentation "Gravité/Vraisemblance", qui regroupe tous les événements redoutés selon leur gravité ainsi que la vraisemblance la plus élevée de tous les scénarios de menaces associés. Ainsi nous obtenons 20 risques, chaque risque correspondant à la perte de l'une des propriétés de sécurité pour un bien essentiel. Ces risques sont classés en fonction de leur vraisemblance et leur gravité dans le Tableau 4.5.

Nous avons défini quatre zones de couleur, indiquant le "niveau" de risque. Par la suite, nous nous intéressons plus particulièrement à la "zone rouge", contenant les risques dont le niveau de gravité est *Critique* et la vraisemblance *Significative*

	Vraisemblance		
Gravité	Minime	Significative	Maximale
Négligeable	PVR non disponible LMR non disponible	TV interactive non disponible	
Limité	VoD non intègre LMR non intègre	VoD non disponible VoD non authentique PVR non authentique	TV non intègre PVR non intègre TV interactive non intègre
Importante		TV non confidentiel TV non authentique VoD non confidentiel PVR non confidentiel TV interactive non confidentiel LMR non confidentiel LMR non authentique	
Critique	TV non disponible	TV interactive non authentique	

Tableau 4.5 – Analyse des risques

ou *Maximale*, ainsi que les risques dont le niveau de gravité est *Important* et la vraisemblance est *Maximale*. Cette zone contient un risque :

— **TV interactive non authentique**, ce risque est directement lié à l'absence de sécurité dans le flux TV aérien ; il n'existe, à ce jour, aucun moyen permettant de vérifier l'authenticité d'un flux TV, et donc du code à exécuter, reçu par un téléviseur.

Nous nous intéressons également à un autre risque, situé dans la zone orange :

— **TV (temps réel) non authentique**, ce risque est lié à l'absence de sécurité du flux TV aérien en général.

Dans la suite de ce chapitre, nous nous intéressons à ces risques par la mise en œuvre technique de plusieurs scénarios de menace à l'origine de ces risques. En effet, en analysant de plus près ces risques, nous retenons deux principaux besoins en sécurité. Premièrement, un besoin d'authenticité du flux TV aérien et des protocoles véhiculés sur celui-ci, et secondement un besoin de confidentialité et d'authenticité sur le lien Internet, véhiculant notamment les mises à jour du firmware.

Pour toutes nos expérimentations, nous avons eu à notre disposition quatre téléviseurs connectés, de différentes marques courantes, représentatifs des téléviseurs connectés vendus en France au moment de l'étude.

La suite de ce chapitre est structurée de la manière suivante. Dans un premier temps, nous discutons du canal TV en présentant d'abord ses spécificités, puis les méthodes et techniques qui nous ont permis d'observer ce canal, et enfin les méthodes et techniques qui nous ont permis une simulation de ce canal. Dans un deuxième temps, nous abordons le protocole HbbTV, d'abord en l'observant puis en le simulant. Dans un troisième temps, nous discutons des phases de mise à jour du firmware. Finalement, dans un quatrième temps, nous présentons nos tests

concernant le respect de la vie privée du téléspectateur.

4.2 Le canal TV

Depuis mars 2005, la France a progressivement basculé toutes ses émissions télévisuelles hertziennes, vers la norme DVB-T. DVB est un ensemble de standards pour la transmission de la télévision numérique [94]. Tout comme pour les précédentes émissions analogiques, il permet l'émission de flux audios et vidéos. La principale nouveauté est la possibilité d'intégrer des flux de données à part entière [5]. En effet, DVB est une extension du flux de transport (TS [6]) MPEG-2 contenant plusieurs flux audios et vidéos ainsi que des flux de données. Ces flux peuvent être acheminés sur différents supports, tels que le satellite, l'aérien ou le câble, respectivement DVB-S, DVB-T et DVB-C. Dans cette étude, nous considérons uniquement la transmission aérienne (DVB-T), qui est le support le plus répandu sur la planète [34].

Dans la suite, nous présentons les techniques existantes afin d'observer le contenu d'un flux DVB. Puis, nous présentons notre plateforme de simulation DVB-T avant d'aborder les premières expériences.

4.2.1 Observation du flux DVB

Le but de ce dispositif est d'observer tous les flux reçus par un téléviseur réglé sur une fréquence en particulier, y compris les flux de données, qui peuvent être invisibles à l'utilisateur. Puisque tous les téléviseurs du marché sont aujourd'hui équipés pour recevoir ces flux, de nombreux outils sont disponibles. Il suffit de se procurer un démodulateur DVB-T, disponible sur étagère. Des outils tels que DVBSnoop [7] permettent ensuite d'effectuer des analyses sur les différents flux élémentaires multiplexés dans un flux de transport DVB, mais également d'enregistrer un multiplex [8] dans sa totalité pendant la durée voulue. Nous avons utilisé également l'utilitaire `tzap` [9] de façon à régler notre démodulateur sur la fréquence souhaitée. Cette démarche est représentée de manière schématique dans la partie "Observation du trafic" de la Figure 4.1. Dans le cadre de l'observation du protocole HbbTV, la Figure 4.3 montre un exemple des sorties du logiciel DVBSnoop.

Il est intéressant de noter que la démarche décrite ici ne remet pas en cause la confidentialité de l'utilisateur. Cependant, on peut considérer la mise en péril de la confidentialité de certaines données appartenant à l'émetteur TV.

5. Dans les émissions analogiques, la transmission de données, comme le télétexte, était possible en utilisant des lignes inexploitées dans le flux vidéo.
6. Transport Stream
7. `http://dvbsnoop.sourceforge.net/`
8. Communication multiplexant plusieurs communications distincts.
9. `http://www.linuxtv.org/wiki/index.php/LinuxTV_dvb-apps`

4.2.2 Plateforme de simulation DVB-T

Ce dispositif est destiné à simuler des émissions de flux de transport DVB [15, 19]. Pour cela, il est nécessaire de posséder un modulateur DVB-T ainsi qu'un multiplexeur de flux MPEG TS, compatible avec le standard DVB. Des applications open-source telles que `ffmpeg` [10] et `vlc` [11], 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. À notre connaissance, en ce qui concerne les logiciels libres, seul l'application Avalpa OpenCaster [12] en est capable.

Comme l'émission de contenus télévisuels 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 spécifique, suggéré par OpenCaster, disponible 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 [13] et QAM16 [14], ce qui réduit grandement la bande passante disponible [15]. Comme la plupart des pays utilisent la modulation QAM64, ce matériel n'est donc pas capable d'émettre entièrement un flux DVB tels que ceux émis en France. Nous avons donc également utilisé une autre plateforme plus chère, mais plus générique et adaptable. Il s'agit d'un matériel permettant de réaliser de la radio logicielle, ou *Software Defined Radio (SDR)*. Nous avons pour cela opté pour le matériel Ettus N210 et sa carte fille WBX. Grâce au logiciel GNU-Radio [16], 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 [25] déjà fonctionnel [17]. A l'aide de ces deux solutions matérielles et du logiciel OpenCaster, nous avons pu implémenter un modulateur DVB-T pleinement fonctionnel.

Le protocole DVB-T est transmis par voie hertzienne. De ce fait, il n'est pas possible de physiquement déconnecter l'émetteur légitime et d'interconnecter 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 suffit d'émettre avec une puissance plus élevée. Bien sûr, dans le cadre de notre expérimentation en laboratoire, 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

10. `https://www.ffmpeg.org/`
11. `http://www.videolan.org/vlc/`
12. `http://www.avalpa.com/the-key-values/15-free-software/33-opencaster`
13. Quadrature Phase-Shift Keying.
14. Quadrature Amplitude Modulation
15. Les différents types de modulations permettent des débits plus ou moins importants en fonction du nombre de symboles définis.
16. `http://gnuradio.org/`
17. Notons que sans ce schéma, nous nous serions heurtés aux mêmes problèmes de traitement du signal que ceux évoqués dans le chapitre précédent.

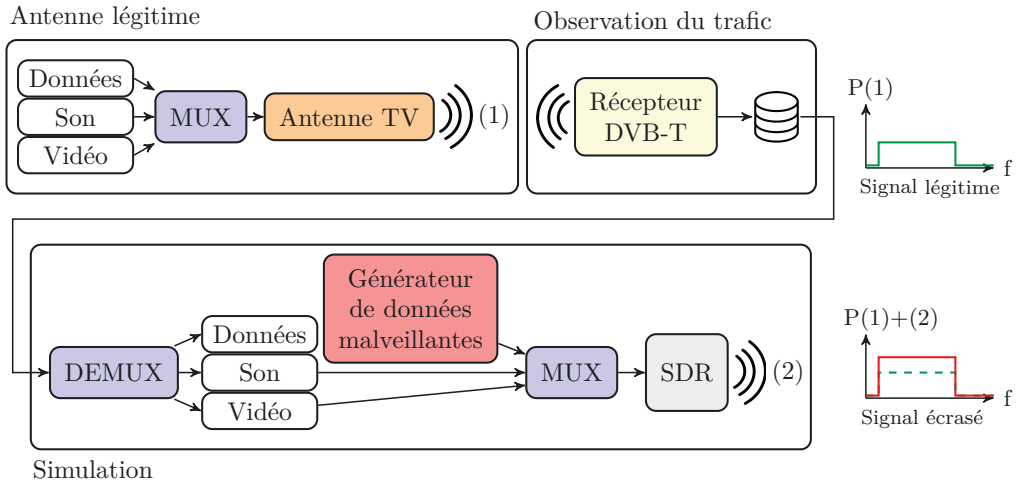


FIGURE 4.1 – Plateforme d'expérimentations DVB

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 [60] de façon à ce qu'un signal plus faible ne puisse interférer avec un signal plus fort. L'ensemble de la plateforme incluant l'émission légitime, l'observation du trafic et la simulation sont représentés dans la Figure 4.1.

Soulignons que les expérimentations, réalisées à l'aide de cette plateforme, ont été menées à l'intérieur de notre laboratoire uniquement, de façon à ne pas perturber d'autres téléviseurs que ceux dédiés à nos expérimentations.

4.2.3 Simulation

Cette première simulation a pour but de valider que notre plateforme est capable d'émettre un flux correct du point de vue du téléviseur. Pour cela, nous avons enregistré un morceau de flux DVB à l'aide de notre solution d'observation (cf. Section 4.2.1). Nous avons ensuite émis ce flux à l'aide de notre plateforme de simulation DVB-T, sans injecter des données malveillantes. Tous les téléviseurs de notre panel d'expérimentation reçoivent et affichent correctement ce signal. Ceci démontre qu'il n'y a aucune vérification de la date d'émission du flux reçu, ni de l'origine du flux.

Afin de démontrer qu'il n'y a pas de vérification d'authenticité d'une émission DVB, nous avons remplacé l'un des flux vidéo, à l'intérieur du multiplex DVB, par un flux capturé à l'aide d'une webcam. Une fois de plus, tous nos téléviseurs reçoivent et affichent correctement le signal émis par notre plateforme.

Nous sommes donc capables d'émettre un flux correct, du point de vue des téléviseurs, et nous savons qu'aucune vérification du contenu n'est effectuée.

4.3 Le protocole HbbTV

Dans cette section, nous nous intéressons à l'émission télévisuelle et à la place qu'elle occupe dans la sécurité des téléviseurs connectés. Nous nous intéressons au fonctionnement et aux impacts de la télévision interactive.

Depuis le basculement vers les standards DVB, les flux télévisuels contiennent de nombreux flux de données. Ces flux permettent, par exemple, de transmettre le résumé du programme en cours. Avec l'arrivée des téléviseurs connectés, différents projets de contenu interactif ont vu le jour. Après plusieurs projets indépendants, la norme HbbTV, *Hybrid Broadcast Broadband TV*, est née en 2010 [48]. Elle est destinée à harmoniser les flux télévisuels et Internet. Ce protocole permet aux chaînes de rajouter du contenu interactif à leur programme TV. L'affichage de ce contenu repose sur l'interprétation d'une page HTML sur le téléviseur du téléspectateur, comme illustré dans la Figure 4.2. L'affichage du contenu initial de HbbTV ne nécessite aucune action de la part du téléspectateur. Cette page est affichée en superposition de l'image de la chaîne regardée, et est souvent constituée d'un petit encadré incitant le téléspectateur à accéder à la suite du contenu, généralement en appuyant sur le bouton rouge de sa télécommande.

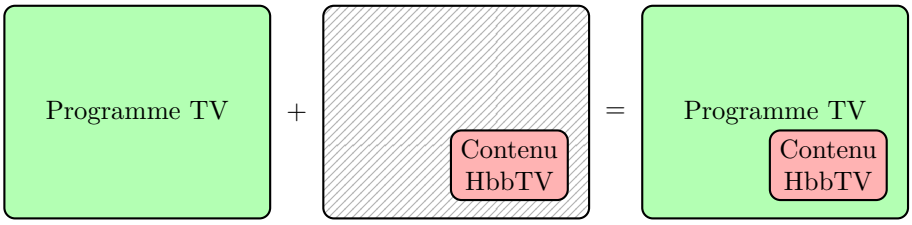


FIGURE 4.2 – Superposition HbbTV

Le protocole HbbTV définit 2 méthodes afin de fournir son contenu au téléviseur :

— En spécifiant l'URL de la page à afficher ; cette solution a pour désavantage de fonctionner uniquement si le téléviseur est connecté à Internet, mais elle permet une gestion plus aisée des mises à jour de la page à afficher.
— En transmettant le contenu de la page à afficher ; cette solution a l'avantage de fonctionner même si le téléviseur n'a pas d'accès à Internet.

4.3.1 Observation du protocole HbbTV

En utilisant la technique d'observation d'un flux DVB, nous sommes également capables d'observer le protocole HbbTV. En effet, chaque flux à l'intérieur d'un

```
Sync-Byte 0x47: 71 (0x47)
Transport_error_indicator: 0 (0x00)  [= packet ok]
Payload_unit_start_indicator: 1 (0x01)  [= Packet data starts]
transport_priority: 0 (0x00)
PID: 170 (0x00aa)  [= ]
transport_scrambling_control: 0 (0x00)  [= No scrambling of TS packet payload]
adaptation_field_control: 1 (0x01)  [= no adaptation_field, payload only]
continuity_counter: 1 (0x01)  [= (sequence ok)]
    Payload: (len: 184)
        ==> pointer_field: 0 (0x00)
        ==> Section table: 116 (0x74)  [= MHP- Application Information Table (AIT)]
    Data-Bytes:
          0000:  00 74 f0 78 00 10 c9 00  00 f0 00 f0 6b 00 00 00   .t.x........k...
          0010:  58 00 02 01 f0 62 02 34  00 03 00 2f 68 74 74 70   X....b.4.../http
          0020:  3a 2f 2f 72 6f 75 74 65  72 2e 68 62 62 74 76 2e   ://router.hbbtv.
          0030:  66 72 61 6e 63 65 74 76  2e 66 72 2f 3f 63 68 61   francetv.fr/?cha
          0040:  69 6e 65 3d 66 72 61 6e  63 65 32 00 01 10 66 72   ine=france2...fr
          0050:  00 0c 46 32 20 42 65 74  61 20 54 65 73 74 16 01   ..F2 Beta Test..
          0060:  00 00 09 05 00 00 01 01  01 ff 01 00 15 0a 69 6e   ..............in
          0070:  64 65 78 2e 68 74 6d 6c  cc 22 77 82 ff ff ff ff   dex.html."w.....
          0080:  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff   ................
          0090:  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff   ................
          00a0:  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff   ................
          00b0:  ff ff ff ff ff ff ff ff                           ........
```

FIGURE 4.3 – Table AIT pour France 2

multiplex est identifié grâce à un identifiant nommé PID [18]. DVBSnoop par exemple permet d'identifier chaque PID d'un multiplex ainsi que son contenu. La Figure 4.3 montre le résultat de l'exécution de DVBSnoop pour le PID 170 du multiplex émis à Toulouse sur la fréquence 746MHz. Ce PID correspond à la table de données "AIT" pour *Application Information Table* de la chaîne France 2. C'est cette table qui véhicule les données HbbTV. En effet, nous pouvons noter l'URL suivante dans les données : `http://router.hbbtv.francetv.fr/?chaine=france2`.

4.3.2 Simulation du protocole HbbTV

Les données HbbTV sont multiplexées à l'intérieur d'un flux DVB. Ainsi, pour simuler le protocole HbbTV, il faut émettre un flux DVB complet. La simulation du protocole HbbTV revient donc à émettre un flux DVB pré-enregistré et non-modifié. Nous avons réalisé cette expérience à l'aide de notre simulateur DVB-T. En observant les requêtes sortant du téléviseur vers Internet, nous avons pu vérifier le bon fonctionnement du protocole HbbTV.

4.3.3 Tentative d'attaque sur le protocole HbbTV

Grâce à nos plateformes d'observation et de simulation DVB-T (cf. Figure 4.1), nous sommes capables d'extraire le flux HbbTV légitime et d'injecter un flux HbbTV modifié. Dans un premier temps, nous avons extrait le flux HbbTV d'un enregistrement réalisé au préalable sur une chaîne existante. Dans un deuxième temps, nous y avons inséré un flux HbbTV contenant une URL pointant vers une page HTML, sur Internet, créée par nos soins. Contrairement aux pages HbbTV habituelles, cette page occupe tout l'écran. A l'aide de notre plateforme d'émission, nous avons émis ce flux afin de l'observer sur les quatre téléviseurs de notre panel d'expérimentation.

18. Packet IDentifier

Les quatre téléviseurs affichent correctement cette page HTML et la vidéo du programme TV en cours n'est plus visible. Ceci montre que les différents téléviseurs n'authentifient pas la source du contenu HbbTV affiché sur leurs écrans. De plus, l'affichage du contenu HbbTV n'est pas limité à une zone spécifique de l'écran et permet d'occulter entièrement la vidéo de la chaîne TV regardée, réalisant ainsi une attaque par déni de service. Dans la suite de cette section, nous abordons d'autres types d'attaques via HbbTV grâce à l'utilisation de JavaScript.

4.3.4 Contenu des pages HbbTV

Après observation du contenu des pages HbbTV légitimes reçues par les téléviseurs, nous nous sommes aperçus que ces pages utilisent du JavaScript afin d'afficher des animations, et également pour intercepter les actions de la télécommande, comme l'utilisation de touches particulières, qui permettent d'accéder au reste du contenu interactif. Alors que JavaScript est massivement utilisé sur le Web, des parties de sa conception et d'intégration laissent, aujourd'hui encore, à désirer [36].

L'un des nombreux problèmes liés à JavaScript est sa capacité d'interroger d'autres pages Web. Étant donné que le code JavaScript est exécuté sur le navigateur client, il bénéficie automatiquement de l'environnement de celui-ci. Ceci signifie qu'il est capable, par exemple, de profiter de l'authentification sur un site distant enregistré dans l'environnement du navigateur. Ainsi, théoriquement, du code JavaScript provenant d'un site accessible depuis `domaine-a.tld` est capable d'agir en tant qu'utilisateur du navigateur sur le `domaine-b.tld`, dès que l'utilisateur accède au site hébergé sur `domaine-a.tld`.

Afin d'empêcher ce comportement, la majorité des navigateurs respectent aujourd'hui la politique de la même origine (*same-origin policy* [85]). 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. La politique 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 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*) 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, telle que représentée dans la figure 4.4.

4.3.5 Respect de la politique de la même origine

Après ces observations, nous avons voulu vérifier le respect de la politique de la même origine par le téléviseur, et plus précisément, par le navigateur intégré qui traite les données HbbTV incluses dans les flux DVB. 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

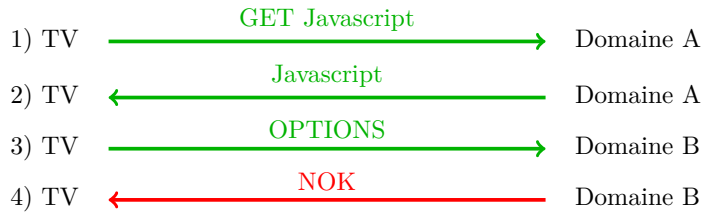


FIGURE 4.4 – Navigateur Web conforme à la politique de la même origine

requête de type HTTP POST sur un site Web différent. Nous avons ensuite multiplexé dans la partie HbbTV du flux DVB, une URL pointant sur ce site Internet. Nous avons testé cette politique de la même origine sur nos quatre téléviseurs, les résultats sont décrits dans le tableau 4.6.

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

Tableau 4.6 – Smart-TV et la politique de la même origine

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", le téléviseur B a une attitude différente en ignorant simplement la requête. En revanche, le 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 multiplexée dans le flux DVB. Ce cas est plus complexe, car le navigateur du téléviseur qui reçoit cette page ne la 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 [81] 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* [48, S6.3] peut être positionné par l'émetteur DVB. Cette variable fait alors office d'origine. Nous avons testé cette politique de la même origine avec nos 4 téléviseurs en définissant ce paramètre et en insérant directement 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 té-

léviseurs, concernant le respect de la politique de la même origine, est identique au cas précédent. Le téléviseur A ne l'implémente pas correctement.

4.3.6 Exploitation du non respect de la politique de la même origine

Nous avons ensuite cherché à exploiter la vulnérabilité du téléviseur A en développant un code JavaScript conçu pour interagir avec l'UAI sur laquelle une Smart-TV est en principe connectée au domicile. L'objectif de cette attaque est d'autoriser sur l'UAI 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 UAI, 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 requêtes UPNP, l'activation d'une 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 envoyé la requête UPNP vers l'UAI. La majorité des UAI déployées en France sont aujourd'hui livrées avec le service UPNP activé par défaut, 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 4.5.

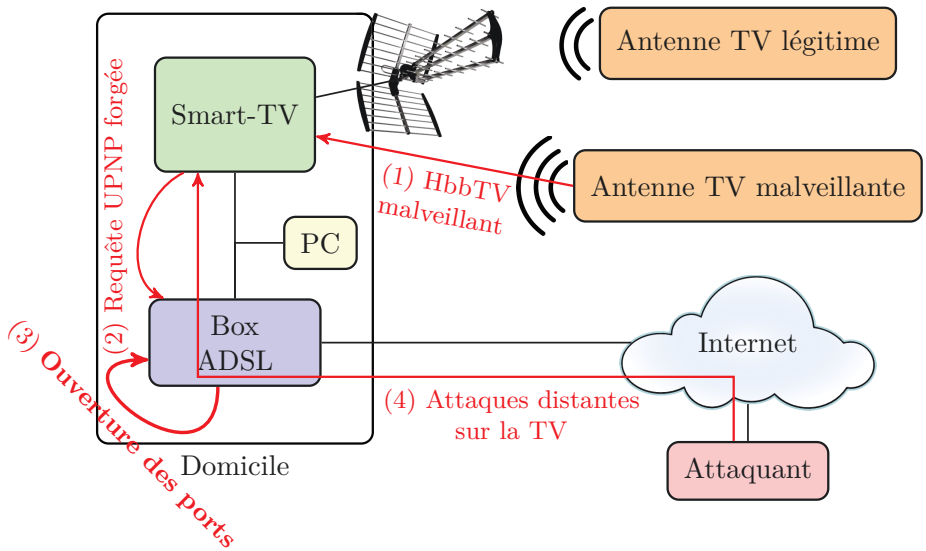


FIGURE 4.5 – Attaque combinée

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 exécutées 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 donc pu 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 [20] et [21]. 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 les téléviseurs.

4.3.7 Vérification du navigateur intégré

Aujourd'hui, les téléviseurs connectés possèdent également un navigateur interactif intégré permettant d'accéder à n'importe quel site Web grâce à un clavier branché sur le port USB du téléviseur. Suite au constat du non respect de la politique de la même origine par l'interpréteur HbbTV, nous avons voulu vérifier le respect de cette politique par ce navigateur Web interactif intégré dans nos téléviseurs. En effet, il est possible que celui-ci n'ait pas le même comportement que l'interpréteur HbbTV. De ce fait, il est possible que ce navigateur ne présente pas les mêmes vulnérabilités. Pour cela, nous nous sommes rendus sur notre site Web contenant du code JavaScript malveillant, en utilisant ce navigateur. Les résultats de cette expérience sont présentés dans le Tableau 4.7.

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

Tableau 4.7 – Navigateur du Smart-TV et la politique de la même origine

Alors que le téléviseur D respectait entièrement la politique de la même origine, il ne la respecte désormais plus du tout. On remarque également, que le téléviseur A respecte désormais la politique, alors que ce n'était pas le cas lors de notre précédente expérience. Aussi, le téléviseur B, même s'il respecte toujours la po-

litique, se comporte différemment. Ceci signifie qu'au moins les téléviseurs A, B et D n'utilisent pas le même interpréteur pour leur navigateur interactif que pour l'interpréteur HbbTV.

4.4 Procédure de mise à jour de firmware

Dans cette section, nous nous intéressons à la procédure de mise à jour du firmware des téléviseurs. Dans notre premier cas d'étude concernant les UAI, nous avons constaté que les protocoles utilisés lors de cette procédure ne sont pas toujours sécurisés et nous voulons ainsi vérifier ces mêmes protocoles pour les téléviseurs.

4.4.1 Observation des procédures de mise à jour

Afin d'observer les procédures de mise à jour des firmware des différents téléviseurs, nous avons utilisé notre plateforme d'observation de communications sur une boucle locale (cf. section 3.2.2). Contrairement aux UAI, pour lesquels il était impératif d'utiliser cette plateforme, il est également possible d'utiliser un hub lorsqu'on a directement accès au réseau local sur lequel est connecté le téléviseur. Cependant, l'utilisation d'un hub permet uniquement d'observer la mise à jour de son propre téléviseur, contrairement à l'utilisation de notre plateforme qui permet d'observer la mise à jour d'un téléviseur d'autrui. En effet, les travaux dans cette thèse s'intéressent plus particulièrement aux attaques réalisables à distance. Ainsi, nous avons observé le trafic lors de ces procédures pour nos quatre téléviseurs, que nous avons reporté dans le Tableau 4.8.

TV		*A*	*B*	*C*	*D*
Négociation	protocole	HTTP	HTTP,HTTPS	HTTPS	HTTP
	contenu	Inconnu	XML,n/a	n/a	XML
Transfert	protocole	HTTP	n/a	HTTP	HTTP
	contenu	Binaire	n/a	Binaire	Binaire

Tableau 4.8 – Procédures de mise à jour des firmwares des téléviseurs connectés.

Pour chaque procédure de mise à jour, nous avons constaté l'existence de deux phases : premièrement, une phase de "négociation" vérifiant la présence d'un nouveau firmware ; puis, lorsqu'une nouvelle version est disponible, une phase de "transfert", pendant laquelle la nouvelle version du firmware est effectivement téléchargée. Pour chaque phase, nous avons identifié les protocoles utilisés ainsi que le type de contenu. Les phases de négociation des téléviseurs A, B, et C sont très similaires, elles utilisent soit le protocole sécurisé HTTPS, auquel cas le contenu est chiffré et donc illisible (référencé n/a dans le Tableau 4.8), ou, lorsqu'un protocole non-sécurisé est utilisé, comme HTTP, le contenu utilise un format inconnu et est également illisible. La phase de négociation du téléviseur D utilise le protocole non-sécurisé HTTP et son contenu est au format XML. Ceci permet à un attaquant

de substituer l'URL du nouveau firmware et ainsi forcer le téléviseur à télécharger un autre firmware. Lorsque la phase de négociation utilise un protocole sécurisé comme HTTPS ou un format inconnu, il devient difficile de déterminer la phase de transfert. Cependant, à part pour le téléviseur B, toutes les phases de transfert utilisent le protocole non-sécurisé HTTP, ce qui permet des attaques de type *man-in-the-middle*. Seule la phase de transfert du téléviseur B est indéterminable (n/a).

4.4.2 Simulation des procédures de mise à jour

Afin de simuler la requête de téléchargement du firmware lors des phases de transfert, nous nous sommes interposés entre le téléviseur et l'UAI. Grâce à un serveur HTTP, nous avons proposé des mises à jour légitimes, mais anciennes [19]. Les téléviseurs A et C ont refusé notre firmware anti-daté sans spécifier de raison. Il est fort probable qu'une signature soit échangée lors de la phase de négociation. Le téléviseur D a accepté notre firmware anti-daté. Cependant, ce firmware est signé, il nous a donc été impossible de le modifier afin d'effectuer une attaque. Cette situation est toutefois problématique dans la mesure où les firmware anti-datés peuvent contenir des vulnérabilités corrigées dans les versions à jour. Ainsi, le passage vers une version antérieure du firmware peut permettre à un attaquant d'exploiter des vulnérabilités normalement corrigées.

4.5 Vie privée

Le respect de la vie privée (*privacy* en anglais) est aujourd'hui une préoccupation grandissante des différents acteurs de la sécurité informatique et il est désormais considéré dans les analyses de sécurité. En particulier, l'utilisation d'Internet, la navigation sur ce réseau, le partage de documents, la participation à des forums ou des réseaux sociaux, font que la vie privée de chacun est constamment mise en danger. Les téléviseurs connectés, reliés au réseau Internet, sont probablement également un bon moyen de véhiculer des informations concernant l'utilisateur, notamment ses habitudes télévisuelles, que l'on peut légitimement considérer comme privées. Il semble donc intéressant d'étudier dans quelle mesure des informations privées peuvent être véhiculées par les téléviseurs, et vers quelle destination.

Nous avons mené trois études concernant :

— la fuite d'informations liées à l'identification des chaînes de télévision effectivement regardées par un utilisateur ;
— la fuite d'informations liées à la connexion au téléviseur de supports de stockage (clés USB ou disques durs) contenant des informations privées ;
— l'utilisation et le stockage des cookies dans l'interpréteur HbbTV du téléviseur.

Nous décrivons ces trois études dans les sections suivantes.

19. Nous avons téléchargé et archivé des firmwares légitimes à partir des sites Web des constructeurs.

4.5.1 Première étude : identification de l'activité de l'utilisateur

Pour cette étude, nous avons mis en place un simulateur de télécommande, afin de dérouler automatiquement un scénario de visionnage sur les téléviseurs. Dans un premier temps, nous présentons ce simulateur. Puis, dans un second temps, nous présentons le scénario de visionnage que nous avons déroulé sur nos téléviseurs. Finalement, nous présentons les résultats de cette étude.

4.5.1.1 Simulateur de télécommande

Les télécommandes des quatre téléviseurs en notre possession utilisent un protocole fondé sur une communication infrarouge (IR). La lumière infrarouge ne permet que deux états, allumé ou éteint. Chaque fabricant de téléviseur peut ensuite utiliser son propre protocole, ou l'un des nombreux protocoles de communication binaire. Par exemple, le fabricant Philips a mis au point un protocole nommé RC5, fondé sur un codage Manchester [20]. Ce protocole utilise 14 bits et permet, au total, de différencier 2048 commandes.

Tout comme pour les téléviseurs, nous avons utilisé des capteurs infrarouge. Ces capteurs absorbent les photons émis par la télécommande et génèrent un flux électrique. Grâce à un Arduino, nous avons pu aisément observer et mesurer la durée de ces flux électriques et les stocker dans une base de données. Nous avons répété cette opération pour les principales touches de chaque télécommande.

Afin de simuler une télécommande, il suffit de reproduire la même séquence de lumière infrarouge produite par les télécommandes. Pour cela, nous avons de nouveau utilisé un Arduino, qui est capable de commander une LED IR. Grâce aux multiples sorties de l'Arduino, nous avons pu connecter quatre LEDs IR, et ainsi contrôler simultanément les quatre téléviseurs de notre panel.

4.5.1.2 Scénario de visionnage

Les scénarios de visionnage que nous avons déroulés simultanément sur les quatre téléviseurs sont représentés dans le Tableau 4.9. Ce tableau représente pour chacune des journées de notre expérience l'activité du téléspectateur. Plus précisément, la présence d'un carré rouge dans la figure indique que le téléspectateur change de chaîne toutes les 15 minutes. La présence d'un carré blanc indique que le téléviseur reste allumé mais qu'il n'y a pas de changement de chaîne.

Ce scénario a pour objectif de représenter différents types d'activités organisées chronologiquement comme suit :

— Activité de référence (jour 1) ; contenant trois périodes rouges de 2,4 et 3 heures respectivement, réparties dans la journée. Elle vise à simuler un scénario dans lequel le téléspectateur est actif devant son téléviseur en début de matinée, puis à la mi-journée et enfin le soir.

— Sans activité / pleine activité / ½ activité (jours 2, 3 & 4) ; ces trois jours sont destinés à représenter 3 profils différents (aucun changement de chaîne

20. 1 → transition haut vers bas, 0 → transition bas vers haut.

	créneau																							
jour	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1									■	■			■	■	■	■				■	■	■		
2																								
3	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
4	■	■	■	■	■	■	■	■	■	■	■	■												
5									■	■			■	■	■	■				■	■	■		

■ = zap tous les 15 min □ = pas d'activité

Tableau 4.9 – Scénarios d'activité de télévision

pendant 24 heures pour le jour 2, changement de chaîne toutes les 15 minutes pendant 24 heures pour le jour 3, changement de chaîne toutes les 15 minutes lors des 12 premières heures, et aucune activité lors des 12 dernières heures pour le jour 4).

— Rejeu de l'activité de référence (jour 5) ; dans le but de vérifier si deux activités identiques espacées de plusieurs jours provoquent les mêmes effets ou pas.

4.5.1.3 Résultats

Globalement, tous les téléviseurs utilisent des protocoles standards : DNS, HTTP et HTTPS. Il est possible que les flux HTTPS contiennent des données relatives à l'activité de l'utilisateur, cependant l'utilisation d'une méthode de chiffrement ne nous permet pas d'analyser ces données. La Figure 4.6 représente le nombre de paquets sortants sur la connexion Internet, par minute, durant cette expérience pour chaque TV. Sur ces graphiques, l'activité de l'utilisateur est représentée en rouge. On remarque très clairement, pour les téléviseurs B et C, que le trafic sortant est corrélé à l'activité de l'utilisateur. Ces graphiques permettent également de constater un profil de données très varié et différent selon la marque du téléviseur. En effet, la différence d'échelles met en évidence un écart très important dans la quantité de données échangées. Ces écarts peuvent en partie s'expliquer par différents phénomènes, notamment par la différence de comportement des navigateurs intégrés aux téléviseurs. En effet, ceux-ci ont la capacité de conserver dans une mémoire cache, pendant une durée définie, le contenu des pages Web. On peut également expliquer ces écarts par une différence de comportement entre les firmwares utilisés respectivement par ces 4 téléviseurs. Certains fabricants mettent à disposition un catalogue d'applications et de widgets [21] disponibles pour ses téléviseurs. Ces applications sont régulièrement mises à jour. En somme, l'analyse du trafic sortant du téléviseur nécessite un travail approfondi, que nous n'avons pas pu mener par faute de temps et qui fait partie des perspectives de cette thèse.

Le téléviseur A a un comportement très différent d'une expérimentation à l'autre. Notons que nous n'avons réalisé aucun paramétrage spécifique sur ces téléviseurs, et que nous avons restauré les paramétrages d'usine après chaque expéri-

21. Applications supplémentaires

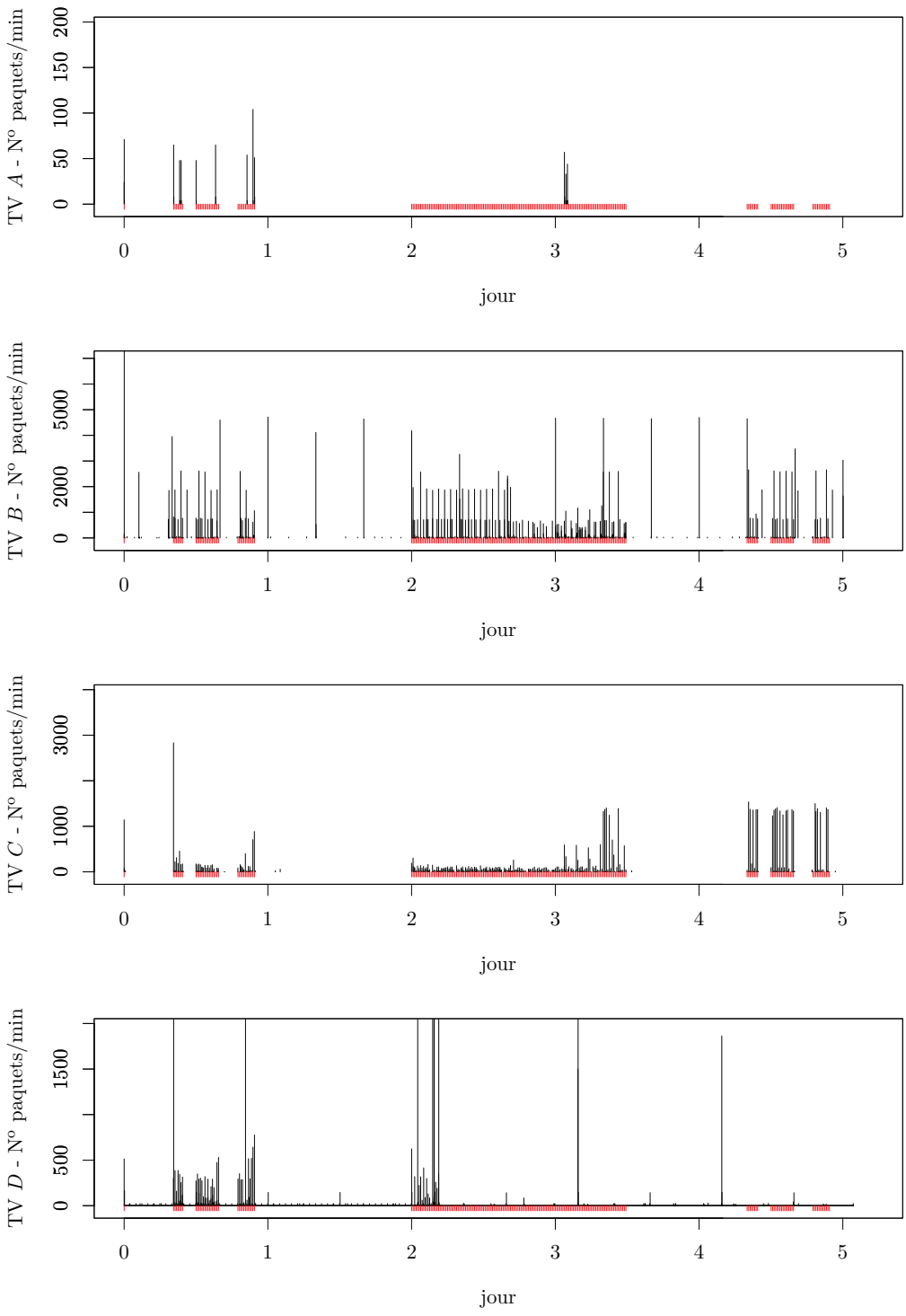


FIGURE 4.6 – Nombre de paquets sortant sur Internet

TV	Fabricant	Chaîne TV	Site statistique	Autre
A [22]	*60%*	*0%*	*0%*	*40%*
B	43%	46%	7%	4%
C	1%	62%	20%	17%
D	9%	72%	10%	9%
Total	17.7%	60%	12.3%	10%

22. Le fonctionnement du téléviseur *A* se révèle très aléatoire, c'est pourquoi nous avons décidé de ne pas prendre en compte ses résultats dans le calcul du total.

Tableau 4.10 – Répartition des requêtes HTTP.

mentation.

Le Tableau 4.10 représente la répartition des requêtes HTTP effectuées par nos 4 téléviseurs. Nous nous apercevons que près de la moitié des requêtes HTTP effectuées sont à destination des sites Internet des chaînes TV. Ces requêtes correspondent à la récupération des pages HbbTV. Les accès au site du fabricant correspondent aux mises à jour du firmware et des widgets. Aucune donnée relative à l'activité du téléspectateur n'a été détectée dans ces communications.

Nous avons observé, à plusieurs reprises, des accès vers les sites `xiti.com` et `google-analytics.com`, qui correspondent à des services de mesure d'audience et de statistique en ligne. Grâce aux *referer*s [23] inclus dans ces requêtes, nous avons pu déterminer que ces requêtes sont toutes provoquées par les pages HbbTV des différentes chaînes TV. De ce fait, on peut déjà supposer que ces données peuvent être, par la suite, transmises aux chaînes TV respectives, puisque ce sont ces chaînes qui utilisent les sites permettant de mesurer l'audience. L'analyse du contenu de ces requêtes, envoyées systématiquement à chaque requête HbbTV, permet de découvrir un certain nombre d'informations concernant le téléviseur dont ils proviennent, comme la marque et l'année de modèle du téléviseur ou encore la résolution de l'image. Si toutes ces données ne révèlent pas d'informations à caractère privé a priori, l'adresse IP contenue dans chaque requête permet de remonter aisément au détenteur de l'UAI derrière laquelle est connecté le téléviseur. Ainsi, ces données peuvent servir à un profilage de l'utilisateur. De plus, nous n'avons aucune preuve que ces données ne sont pas stockées pour un usage ultérieur par le site de mesure d'audience et de statistique en ligne ou les chaînes TV commanditaires de cette collecte d'informations. Ceci semble en partie être confirmé par des études récentes, comme [43], qui montrent comment certains téléviseurs envoient le nom de la chaîne regardée par le téléspectateur vers un site du fabricant du téléviseur. L'un de nos quatre téléviseurs est de la même marque que celui visé dans l'article, mais de modèle différent et nous n'avons pas, a priori, constaté le même comportement que celui décrit dans cette étude.

Les requêtes "Autre" regroupent toutes les requêtes dont ni l'URL, ni le contenu

23. Lorsqu'une requête est générée par une page, le navigateur inclut un *referer* dans la requête permettant de déterminer l'origine de la requête.

des échanges ne nous ont permis de les classer parmi les trois catégories précédentes. Si toutefois, nos quatre téléviseurs ne divulguent, a priori, pas directement l'activité du téléspectateur, l'analyse du trafic sortant sur Internet permet de le déterminer.

4.5.2 Deuxième étude : connexion de périphériques de stockage

Les téléviseurs connectés, qui contiennent aujourd'hui des firmwares très riches, intègrent des lecteurs capables de lire des fichiers multimédia contenus sur des périphériques de stockages ou téléchargés depuis le réseau local ou depuis le réseau Internet. Étant donné que les périphériques de stockage, comme les clefs USB ou les disques durs externes, contiennent fréquemment d'autres fichiers à caractère privé, nous avons voulu vérifier que nos téléviseurs ne s'intéressaient pas à ces fichiers.

Pour cette étude, nous avons analysé le trafic sortant sur Internet de chaque téléviseur pendant le branchement d'une clef USB contenant plusieurs fichiers multimédia, ayant comme nom de fichier `Oblivion.2013.FRENCH.BDRip.x264-AYMO.mkv` ou `FriendsS01e01.avi`, ainsi que des documents factices ayant pour nom de fichier `privé.pdf` ou encore `motdepasse.txt`. Pour chaque TV, nous avons laissé la clef USB branchée pendant 24h avant de lire certains fichiers contenus sur celle-ci.

Si la lecture de ces fichiers n'a eu aucun impact sur les communications sortantes, et aussi étonnant que cela puisse paraître, l'un de nos quatre téléviseurs a régulièrement émis une requête vers le site de son fabricant contenant un certain nombre de noms de fichiers, aléatoirement choisis parmi ceux présents sur la clef USB branchée sur le téléviseur. La Figure 4.7 présente un extrait de l'une de ces requêtes interceptées entre le téléviseur et le fabricant sur le lien Internet. Sur cet extrait, nous apercevons très clairement, entre autres, la divulgation du nom du fichier factice que nous avons créé, nommé `motdepasse.txt`.

```
00000330                                                  71 75                 qu
00000340  65 72 79 3d 6d 6f 74 64  65 70 61 73 73 65 25 32 ery=motd epasse%2
00000350  45 74 78 74 3a 2f 4f 62  6c 69 76 69 6f 6e 25 32 Etxt:/Ob livion%2
00000360  45 25 33 32 25 33 30 25  33 31 25 33 33 25 32 45 E%32%30% 31%33%2E
00000370  46 52 45 4e 43 48 25 32  45 42 44 52 69 70 25 32 FRENCH%2 EBDRip%2
00000380  45 78 25 33 32 25 33 36  25 33 34 25 32 44 41 59 Ex%32%36 %34%2DAY
00000390  4d 4f 25 32 45 6d 6b 76  3a 2f 46 52 45 4e 43 48 MO%2Emkv :/FRENCH
000003A0  25 35 46 53 63 52 65 45  6e 45 72 25 32 45 6d 6b %5FScReE nEr%2Emk
000003B0  76                                               v
```

FIGURE 4.7 – Extrait d'une requête depuis le téléviseur vers son fabricant

Des travaux similaires [43] pointent du doigt un comportement identique sur un téléviseur de la même marque que celle concernée par nos études. Plusieurs mois après ces expériences, une mise à jour du firmware de ces téléviseurs a été publiée. Désormais ces téléviseurs ne semblent plus communiquer le nom des fichiers contenus sur un périphérique de stockage branché à celui-ci.

Nous n'avons pas effectué d'expériences supplémentaires concernant cet aspect, par manque de temps, mais il serait intéressant d'effectuer des expérimentations du même type en utilisant les autres fonctionnalités des téléviseurs, comme l'enregistreur numérique intégré par exemple. Il est tout à fait possible que les téléviseurs

puissent, d'une façon ou d'une autre, envoyer sur le réseau Internet des informations concernant ces activités d'enregistrement d'émissions du téléspectateur, informations qui peuvent permettre d'établir des profils d'utilisation.

4.5.3 Troisième étude : utilisation et stockage des cookies

Nous avons consulté la Commission nationale de l'informatique et des libertés (CNIL) concernant les aspects légaux du respect de la vie privée. En ce qui concerne ce cas d'étude, le référentiel le plus applicable est leur recommandation sur les cookies et autres traceurs [67].

Ce document stipule que dès lors que les cookies sont utilisés à des fins de mesure d'audience ou de facilitation de la communication par voie électronique, leur utilisation ne nécessite pas de consentement préalable. Cependant, l'article 6 stipule, pour les cookies de mesure d'audience, que : "La personne doit être informée", puis plus globalement, elle doit pouvoir s'y "opposer par l'intermédiaire d'un mécanisme d'opposition facilement utilisable".

En analysant les échanges, nous observons également le dépôt de cookies, principalement issus des sites appartenant aux chaînes, définissant des marquages temporels, et une géolocalisation. On est donc bien dans le cas de cookies de mesure d'audience. En considérant que l'achat d'un téléviseur vaut acceptation des conditions générales de vente du fabricant, il n'en est rien envers les chaînes TV. N'étant pas informé du dépôt de cookies en accédant au contenu HbbTV, notre interprétation nous laisse supposer que les chaînes TV ne respectent pas la législation.

4.6 Conclusion

Avec l'arrivée de l'Internet haut débit, la tendance est au tout numérique. De plus en plus d'équipements grand public sont désormais connectés à Internet afin d'en enrichir le contenu et l'interactivité. Les Smart-TVs en sont, aujourd'hui, un exemple bien concret dans de nombreux foyers. Ces téléviseurs de nouvelle génération reçoivent toujours un flux temps réel par voie hertzienne, mais offrent également à l'utilisateur de nouveaux services comme la vidéo à la demande ou des applications interactives, grâce à leur connexion Internet. De nouveaux protocoles permettent même aujourd'hui de multiplexer dans le flux hertzien des données (comme des pages Web ou des URL de pages Web) destinées à être traitées par le téléviseur grâce à sa connexion Internet. Il devient alors essentiel d'assurer l'authenticité des différents flux utilisés par le téléviseur. Les différentes expériences dans ce chapitre avaient pour but de mettre en évidence un certain nombre de faiblesses, en particulier en ce qui concerne ces différents flux. En suivant la méthode présentée dans le chapitre 2, nous avons ainsi pu mettre en évidence que la sécurité n'est pas encore suffisamment au rendez-vous, du moins pour certains des téléviseurs que nous avons testés.

Les expérimentations menées à travers nos deux cas d'étude ont permis de mettre en évidence des faiblesses dans les différentes procédures de mise à jour

de firmware de plusieurs UAI et téléviseurs que nous avons étudiés dans le cadre de cette thèse. Ce problème est d'autant plus important que le nombre d'objets grand public connectés à Internet est, aujourd'hui, en constante augmentation. En effet, la commission européenne estime, suite à une consultation en 2012 [49] qu'en 2012, chaque utilisateur moyen dispose d'au moins deux objets connectés à Internet et que ce chiffre passera à sept d'ici à 2015. Tous ces objets sont susceptibles d'utiliser Internet afin de mettre à jour leur firmware, et présenter ainsi les mêmes vulnérabilités que celles mises en évidence lors de ces expériences. Dès lors, il devient primordial de se préoccuper de la sécurité de ces équipements et de leurs procédures de mise à jour.

Comme pour les UAI, nous pensons que la majorité des risques identifiés dans ce chapitre peuvent être éliminés ou réduits à l'aide de contre-mesures, simples à mettre en œuvre. Nous les abordons dans le chapitre suivant.

Chapitre 5

Contre-mesures

Sommaire

Les chapitres précédents de ce manuscrit ont essentiellement traité des problématiques de détection de vulnérabilités et d'élaboration de scénarios d'attaque. Il est bien sûr fondamental, avant de terminer ce manuscrit, d'aborder un certain nombre de contre-mesures que nous pouvons envisager pour faire face aux différentes attaques que nous avons expérimentées. Cette recherche de contre-mesures est d'ailleurs directement en relation avec l'analyse des risques que nous avons utilisée dans notre méthode globale puisque la dernière étape d'une analyse des risques concerne le traitement des risques.

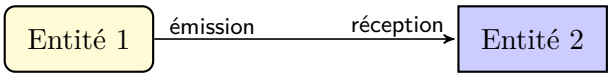
Un grand nombre d'équipements grand public sont aujourd'hui connectés à Internet. C'est pourquoi il devient primordial de ne plus seulement considérer la sécurité des ordinateurs personnels, mais de tous ces équipements connectés à Internet. Dans cette thèse, nous nous sommes focalisés sur des aspects bien particuliers, les communications entre ces équipements et leur fournisseur de services respectifs. Il convient d'aller au-delà et de considérer tous les aspects pouvant impacter la sécurité de ces objets. Nous aborderons ces considérations dans les perspectives à ces travaux.

Ce chapitre est organisé comme suit. Dans un premier temps, à la lumière des expérimentations de cette thèse, nous donnons un aperçu global des éléments principaux des équipements connectés qu'il est nécessaire de sécuriser, puis nous abordons les différents moyens existants pour assurer leur sécurité. Ces éléments à sécuriser

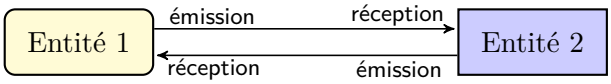
concernant principalement les moyens de communication avec d'autres équipements, nous nous fondons sur les protocoles réseaux existants et sur les mécanismes permettant d'assurer leur sécurité. Ainsi, nous revenons brièvement, dans une seconde partie, sur la définition du modèle OSI et des couches protocolaires. Finalement, nous présentons, pour chacun des cas d'étude et plus précisément, pour chacune des communications vulnérables identifiées, les différents mécanismes de sécurité applicables.

5.1 La sécurisation des moyens de communication

Dans cette thèse, nous nous sommes intéressés à la sécurité des équipements grand public connectés à Internet, et plus précisément à la sécurité de leurs liens de communication. Lors de nos deux cas d'étude, nous nous sommes aperçus que les différents liens de communications et notamment ceux avec leurs fournisseurs de services, n'implémentent pas systématiquement des méthodes permettant d'assurer la sécurité des données. Nous avons ainsi identifié, pour les UAI et les téléviseurs connectés, des problèmes d'intégrité, d'authenticité et de disponibilité. Ces deux cas d'étude sont d'autant plus intéressants qu'ils permettent d'illustrer les deux formes de communication utilisées par les équipements : les communications unidirectionnelles et bidirectionnelles. Ces deux formes de communication sont illustrées dans la Figure 5.1.



Communication unidirectionnelle



Communication bidirectionnelle

FIGURE 5.1 – Communications unidirectionnelles et bidirectionnelles

L'UAI, étudiée lors de notre premier cas d'étude dans le chapitre 3 et son fournisseur de services, le FAI, sont un exemple concret de communication bidirectionnelle. Ces deux entités émettent et reçoivent des messages provenant de l'entité adverse et inversement. Le téléviseur connecté en revanche, étudié lors de notre second cas d'étude, dans le chapitre 4, et son fournisseur de services, l'émetteur TV, sont un exemple concret de communication unidirectionnelle. L'émetteur TV émet des messages à destination du téléviseur, mais le téléviseur n'est pas capable de répondre sur ce canal de communication.

Plus généralement, chaque équipement connecté possède n interfaces de communication (cf. section 1.2.2) permettant d'émettre des informations vers une autre

entité ou de recevoir des informations depuis cette autre entité. D'une manière générale, il convient, pour chacun des liens d'un équipement connecté, d'analyser le besoin par rapport à chaque propriété de sécurité de l'information, à savoir la disponibilité, l'intégrité et la confidentialité. Par extension, l'intégrité des méta-données nous conduit à nous intéresser également à l'authenticité.

Toutefois, chaque propriété de sécurité n'est pas systématiquement requise sur chaque lien de communication. Ainsi, nous considérons que, pour chaque lien, les différentes propriétés de sécurité doivent être envisagées et étudiées. Nous montrons ci-dessous, à l'aide de quelques exemples, comment l'importance des différentes propriétés peut varier d'un cas à un autre.

- Le non respect de la **disponibilité** est plus facilement tolérable dans un environnement grand public que dans un environnement industriel. Cependant, pour certains cas d'application, comme les systèmes d'alarmes ou pour des applications de télémédecine, le facteur disponibilité peut devenir un enjeu primordial. En revanche, à certaines heures de la journée, le fait que le flux télévisuel soit indisponible peut ne pas être catastrophique pour grand nombre d'individus.
- Le non respect de l'**intégrité** est un problème majeur quel que soit l'environnement. En effet, il est difficile d'imaginer un cas de figure où l'altération des données soit acceptable. Nous considérons ici que la non intégrité des méta-données d'une communication, i.e., l'authenticité, est un problème à part.
- Le non respect de la **confidentialité** ne pose problème que lorsque les données transmises doivent être accessibles à une ou plusieurs entités bien définies. Concrètement, il s'agit de données sensibles telles que des identifiants ou un dossier médical par exemple, ou du contenu d'un service payant, comme la VoD. Si l'on envisage le cas de diffusion d'émissions télévisuelles, qui sont émises en broadcast et identiques pour tous les clients, la confidentialité n'est donc pas critique.
- Le non respect de l'**authenticité**, tout comme le non respect de l'intégrité, est également un problème majeur, car en aucun cas il n'est acceptable de ne pas pouvoir identifier l'entité avec laquelle on communique.

Afin d'illustrer cette problématique, prenons l'exemple d'un système d'alarme grand public. Nous considérons que ce système utilise la connexion Internet du domicile afin de communiquer avec la plateforme de surveillance à laquelle l'utilisateur est abonné. Les différents capteurs de détection d'intrusion communiquent leur état, via une liaison sans-fil, au système d'alarme.

Ce système d'alarme possède donc $n = n_c + 1$ liens sortants, avec $n_c =$ le nombre de capteurs de détection d'intrusion. Le premier lien sortant, la connexion Internet entre le système d'alarme (*équipement connecté*) et la plateforme de surveillance (*fournisseur de services*), doit être :

- **disponible** afin d'assurer une surveillance permanente du domicile par la plateforme de surveillance,
- **intègre** afin d'assurer la réception de la bonne information depuis le système

d'alarme permettant une intervention en cas de compromission du domicile,
— **confidentiel** afin de ne divulguer aucune information sur l'activité de l'utilisateur *(présence ou absence du domicile)* à une entité tierce, et
— **authentique** afin de garantir à la plateforme de surveillance qu'elle reçoit bien les informations depuis le bon système d'alarme, et non de celui d'une entité malveillante.

Les n_c liens entre le système d'alarme (*équipement connecté*) et les capteurs (*objets communicants*) respectifs doivent être :
— **disponibles** afin de fournir en permanence au système d'alarme l'information provenant de chaque capteur,
— **intègres** afin d'assurer la réception de la bonne information depuis les capteurs sur le système d'alarme qui doit à son tour communiquer sur une éventuelle intrusion avec la plateforme de surveillance, et
— **authentiques** afin de garantir au système d'alarme qu'il discute avec le capteur légitime et non un capteur malveillant déployé par un attaquant.

Dans ce cas précis nous considérons que l'information provenant du capteur de détection d'intrusion ne nécessite pas de confidentialité. En effet, l'état d'une ouverture (fenêtre, porte, etc.) ne permet pas de déduire d'informations sensibles concernant l'utilisateur.

Grâce à l'identification des besoins sur chaque lien de l'équipement, il est donc possible d'étudier les systèmes de sécurité adaptés. Ces mécanismes sont indépendants pour chaque type d'interface de communication, doivent répondre aux besoins de sécurité identifiés et doivent être compatibles avec les ressources matérielles disponibles à l'intérieur de l'équipement. En effet, dans le cadre de micro-capteurs, par exemple, il est probablement très difficile de mettre en œuvre des mécanismes de chiffrement nécessitant des ressources matérielles et énergétiques importantes, qui seraient trop coûteuses pour la majorité de ces équipements. Pour cette raison, il existe des solutions de sécurité à différents niveaux protocolaires d'une communication.

Dans la suite de ce chapitre, nous rappelons dans un premier temps les concepts du modèle OSI et les piles de protocoles avant de l'appliquer aux canaux de communication étudiés à travers nos deux cas d'étude. Ensuite, nous présentons des contre-mesures concrètes aux différents problèmes de sécurité rencontrés à travers les deux cas d'études de cette thèse.

5.2 Modèle OSI & piles protocolaires

Le modèle de référence OSI [102], illustré dans la Figure 5.2, comporte sept niveaux protocolaires plus un médium physique. Le médium physique, parfois appelé niveau 0, correspond au support physique de communication chargé d'acheminer les informations entre deux équipements sur un réseau. On appelle "pile de protocoles" la suite complète de protocoles utilisée par une entité de la communication. À l'intérieur de cette pile, on distingue deux niveaux de couches protocolaires, pre-

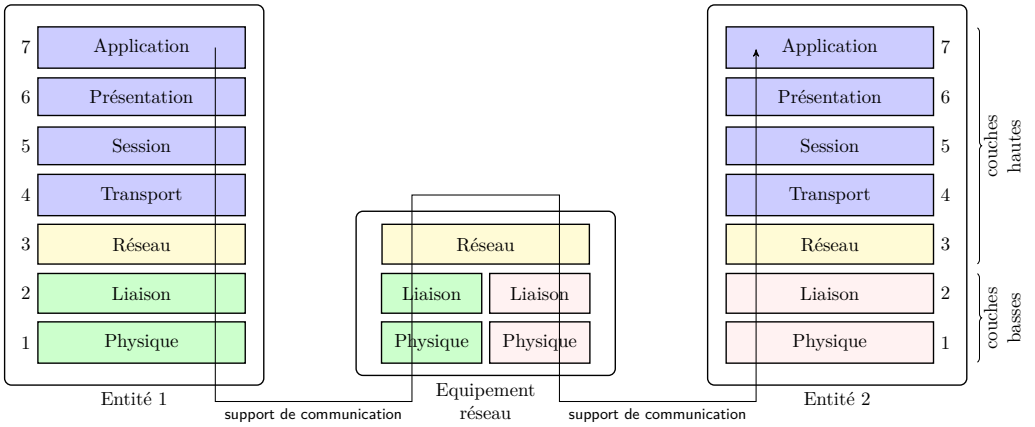


FIGURE 5.2 – Modèle OSI

mièrement, les couches “hautes”, identiques chez les deux entités de la communication et absentes chez les équipements réseau intermédiaires, puis secondement, les couches “basses” dont les protocoles peuvent varier sur chaque tronçon physique de la communication. C’est pourquoi, dans le cadre d’une communication Internet par exemple, la pile de protocoles peut varier sur chaque tronçon du réseau entre l’abonné et les serveurs du FAI.

Les différentes propriétés de sécurité nécessaires à la communication peuvent être assurées à différents niveaux de la pile de protocoles utilisée par la communication. Cependant, les mécanismes de sécurité sur les couches basses sont nécessairement liés à une technologie physique particulière et ne peuvent donc s’appliquer qu’au tronçon concerné par cette technologie, et non sur la communication de bout en bout. Ainsi, chaque communication peut implémenter différents mécanismes de sécurité, fonctionnant à différents niveaux de la pile de protocoles. Ces mesures peuvent être redondantes les unes par rapport aux autres, et peuvent ne pas couvrir la totalité de la communication entre les deux entités.

Dans la suite de ce chapitre, nous revenons sur nos deux cas d’étude en présentant les piles de protocoles mises en œuvre et les mesures de sécurité envisageables sur les différents niveaux protocolaires. En ce qui concerne les contre-mesures sur les couches basses, nous nous intéressons principalement au premier tronçon de la communication du point de vue de l’utilisateur, c’est-à-dire la pile de protocoles présente sur le lien sortant du domicile de l’utilisateur. Pour chaque mécanisme de sécurité envisagé, nous discutons les conditions et les intérêts de la mise en œuvre du mécanisme.

5.3 La connexion au réseau Internet

Nos deux cas d’études, et plus particulièrement celui concernant les UAI, nous ont conduit à étudier la sécurité des boucles locales. La boucle locale, quel que soit

son support physique, est le premier tronçon d'une connexion au réseau Internet. Les différentes expérimentations que nous avons menées nous ont permis de dévoiler un certain nombre de failles de sécurité pour lesquelles il existe différents mécanismes de sécurité. Dans cette section, nous présentons dans un premier temps la pile de protocoles généralement rencontrée sur cette boucle locale avant de présenter, dans un second temps, les différentes contre-mesures aux problèmes de sécurité identifiés.

5.3.1 Pile de protocoles

Le réseau Internet est hétérogène, ce qui signifie qu'il est capable de fonctionner sur un ensemble de réseaux physiques indépendants et différents les uns des autres. Il existe différentes technologies pour relier un domicile au réseau Internet, et pourtant il est possible de communiquer avec n'importe quel utilisateur connecté à Internet, quel que soit le type de réseau d'accès qu'il utilise. Dans le cadre de cette thèse, nous nous sommes focalisés sur les boucles locales ADSL, utilisant majoritairement des réseaux à commutation de cellules, comme ATM par exemple. Ici, nous considérons la pile mise en œuvre par la majorité des opérateurs ADSL implémentant le protocole IP au-dessus de PPP au-dessus d'ATM (IPoPPPoA) (cf. Figure 5.1). Notons qu'on retrouve régulièrement une couche Ethernet entre PPP et ATM.

№	№ OSI	Nom	Description
5	5-7	Application	Couche Application *(http, ftp, ...)*
4	4	Transport	Généralement TCP ou UDP
3	3	IP	Couche réseau
2c	2	PPP	PPP (*Point to Point Protocol*)
2b	2	AAL	Couche AAL (*ATM Adaptation Layer*)
2a	2	ATM	Couche ATM (*Asynchronous Transfer Mode*)
1	1	Physique	Couche physique ou PMD (*Physical Medium Dependant*)

Tableau 5.1 – Exemple de pile Internet (IPoPPPoA)

5.3.2 Les couches hautes

Les couches hautes ont pour avantage d'être présentes de bout en bout de la communication. Ainsi, des mécanismes de sécurité appliqués à ce niveau permettent d'assurer la sécurité sur toute la chaîne de communication entre l'équipement et son fournisseur de services.

5.3.2.1 La couche application

Dans un premier temps, nous nous focalisons sur les données véhiculées par la couche applicative, qui peuvent tout à fait être sécurisées à la discrétion de l'application sans utiliser des mécanismes génériques tels que TLS, que nous aborderons dans la couche suivante. En effet, la modification des données que nous avons pu réaliser lors de nos expérimentations sur les équipements étudiés, a pu l'être en

raison de l'absence de sécurisation de ces données. C'est pourquoi, il est possible de mettre en œuvre, à l'intérieur de chaque application, des mécanismes de chiffrement et de signature des données, ce qui permet ensuite d'utiliser une pile TCP/IP standard sans mécanisme de protection.

En optant pour ce type de mécanisme de sécurité, deux possibilités s'offrent au fabricant. Premièrement, il peut développer lui-même son propre mécanisme de protection à intégrer dans son application. Cette solution est souvent très coûteuse et ne bénéficie pas de l'expérience de la communauté et des applications éprouvées. Il y a donc des risques d'inclure des failles de sécurité. Deuxièmement, il peut utiliser des librairies existantes, dont la résistance a été prouvée dans le temps, et pour lesquelles des mises à jour sont régulièrement disponibles. Cette deuxième option permet de n'intégrer que les fonctionnalitées souhaitées par l'application et d'être ainsi bien plus légère qu'une implémentation complète sur la couche transport.

Dans tous les cas, la sécurisation à ce niveau nécessite une modification importante de l'application, et souvent, une mise à jour de tous les équipements déjà sur le marché. Cette option est donc à privilégier dès la conception de l'équipement, et non en contre-mesure.

On peut également s'intéresser au problème particulier de la protection de la vie privée. Par exemple, dans le cadre des téléviseurs connectés (cf. section 4.5), nous avons abordé le problème de la divulgation de l'activité du téléspectateur, mais on peut imaginer bien d'autres situations dans lesquelles la protection de la vie privée sera un des enjeux principaux. Dans ce cas précis, lorsqu'il n'est pas nécessaire de considérer les autres propriétés de sécurité, il est possible de mettre en œuvre des mécanismes permettant d'anonymiser les données, sans les rendre confidentielles. Ceci signifie qu'une personne extérieure, peut observer l'activité provenant du domicile, sans être capable d'identifier le téléspectateur qui y est associé. Pour cela, lorsque l'équipement n'intègre pas de mécanisme assurant la confidentialité des données, nous pouvons imaginer une autre solution, qui s'applique notamment aux fuites d'informations privées éventuelles des téléviseurs connectés. Cette solution consiste à générer du trafic comparable au trafic légitime afin de tromper une éventuelle entité malveillante observant le trafic sortant du domicile. En effet, la principale motivation dans la collecte des données à caractère privée est l'obtention d'un profil précis de l'individu observé, c'est-à-dire la connaissance précise de ses habitudes personnelles. Ainsi, en générant du bruit parmi les requêtes légitimes, il est possible de fausser le profil obtenu par un attaquant. Il est possible pour cela d'envoyer des données de façon aléatoire (ce qui peut être détecté assez facilement) mais on peut imaginer également utiliser une plateforme collaborative afin d'échanger des séquences de comportement de différents individus et de pouvoir ainsi rejouer chez soi le comportement d'une autre personne. Ceci peut éviter la détection d'un flux aléatoire.

L'avantage d'une telle solution est de permettre à l'utilisateur d'anonymiser lui-même son activité lorsque l'équipement n'implémente pas des mécanismes permettant de réaliser cette tâche.

5.3.2.2 Les couches transport et session

Sur Internet, la majorité des protocoles de la couche application reposent sur TCP ou UDP. Le protocole UDP fournit, contrairement au protocole TCP, un service en mode sans connexion et sans reprise en cas d'erreur. Seule l'utilisation du protocole TCP permet, nativement, de détecter des modifications des données échangées de bout en bout lors de perturbations d'origine accidentelle, grâce à un code de contrôle.

L'une des principales failles de sécurité rencontrées à travers l'étude des UAI et des téléviseurs connectés est l'utilisation de protocoles de niveau applicatif comme HTTP ou FTP sans utilisation des mécanismes de sécurité offerts par la couche transport. La sécurisation des protocoles applicatifs par Transport Layer Security (TLS), pour *sécurité de la couche de transport*, permet d'assurer l'`Authenticité`, l'`Intégrité` et la `Confidentialité` des protocoles applicatifs.

Pour cela, la couche TLS propose un mécanisme de chiffrement symétrique entre les deux entités de la communication. Ce chiffrement utilise une clé symétrique que les deux entités s'échangent de façon sécurisée, grâce à l'utilisation de chiffrement asymétrique et de couples de clés privée/publique appartenant à chaque entité. Ces clés sont délivrées sous forme de certificats numériques à l'aide d'une infrastructure de clés publiques (PKI pour *Public Key Infrastructure*) et d'autorités de certification.

Cependant, pour que TLS soit efficace, son implémentation doit être rigoureuse. En effet, il faut veiller à correctement valider les certificats présentés lors de la phase de négociation. Ces certificats permettent, s'ils sont issus d'une autorité de certification (AC) de confiance, de valider l'authenticité des deux entités de la communication. Il est donc essentiel de pouvoir accorder une confiance totale à celle-ci. De plus, une AC doit également proposer un système permettant de révoquer des certificats, en cas de compromission par exemple. Classiquement, tout navigateur Internet intègre une liste des AC de confiance, ainsi, la visite sur un site présentant un certificat non-conforme nous demande d'accepter ou de refuser le certificat présenté et de poursuivre ou non la communication. Dans de très nombreux cas aujourd'hui, seul le certificat de l'entité serveur est vérifié par le client ; le client de son côté possède rarement un certificat. Or, il est possible d'exiger du serveur de vérifier le certificat présenté par le client et instaurer ainsi une authentification mutuelle. Enfin, il convient également de respecter les recommandations émises par l'entité étatique responsable de la sécurité des systèmes d'informations du pays [71], soit l'ANSSI en France, qui propose régulièrement un état des lieux des protocoles de chiffrement utilisables et conseillés dans notre pays.

La Figure 5.3 présente une attaque du type "homme du milieu" lorsque le client ne vérifie pas le certificat émis par le serveur. Dans ce cas, l'attaquant est capable de lire les données échangées entre le client et le serveur.

La Figure 5.4 présente une autre attaque, dans le cas où le serveur ne vérifie pas le certificat émis par le client. La vérification du certificat client par le serveur permet au serveur de n'autoriser les communications, et donc l'échange de données, qu'avec

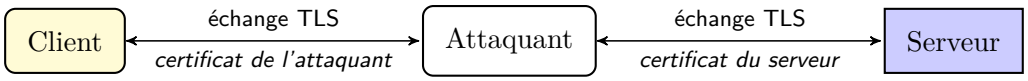


FIGURE 5.3 – Man in the middle TLS

des clients légitimes et authentifiés. Par exemple, dans le cadre d'une procédure de mise à jour d'un équipement connecté, la vérification du certificat client permet au fabricant de s'assurer que le firmware n'a pas été téléchargé par un attaquant afin d'en analyser le contenu. Lorsque le serveur ne vérifie pas ce certificat client, comme le montre la Figure 5.4, un attaquant est ainsi capable de se faire passer pour un client légitime et peut accéder à des données qui étaient destinées uniquement à certains clients.

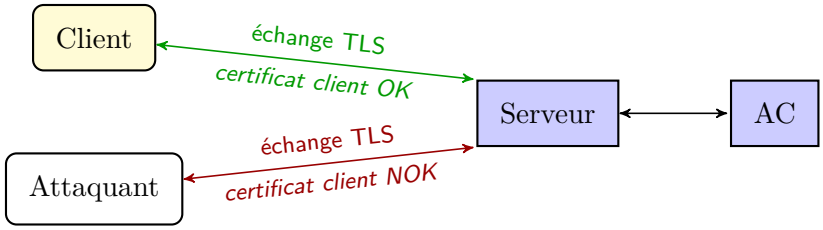


FIGURE 5.4 – Vérification du certificat client

Cependant, comme tout code informatique, il est possible que certaines implémentations de TLS contiennent des vulnérabilités. A ce propos, en 2014, plusieurs révélations ont marqué l'histoire de TLS. Notamment en mars, avec la vulnérabilité `Heartbleed` [45], présente dans la librairie `OpenSSL`, qui permet à un attaquant de lire une partie de la mémoire du serveur ou du client, contenant potentiellement des informations sensibles, comme par exemple les clefs de chiffrement. C'est pourquoi il convient de suivre l'actualité concernant les mécanismes de sécurité mis en œuvre, et si possible, d'implémenter un autre mécanisme à un niveau protocolaire différent.

Alors que c'est loin d'être le cas aujourd'hui, nous considérons qu'il est primordial d'implémenter TLS sur tous les équipements grand public connectés à Internet. Cependant, l'implémentation de TLS est relativement lourde et nécessite des ressources de calcul non négligeables. Dans le cadre des objets connectés en général, il n'est probablement pas envisageable de pouvoir embarquer TLS systématiquement dans leur code. Pour certains objets de fine granularité, possédant peu de ressources mémoire et CPU, il semble très difficile d'implémenter une couche TLS. D'autres mécanismes de sécurité peuvent alors mieux convenir. Pour des objets tels que des micro-capteurs, n'implémentant pas les couches "hautes" du réseau, il est également nécesssaire d'envisager des mécanismes de protection dans d'autres couches protocolaires. Cependant, en ce qui concerne les équipements que nous avons étudiés dans cette thèse, et qui disposent en général de puissance et de mémoire suffisante, et qui intègrent toutes les couches du modèle OSI, l'utilisation de TLS nous semble

très vivement recommandée.

5.3.2.3 La couche réseau

La couche réseau, implémentant le protocole IP assure l'acheminement des trames provenant d'une entité vers l'autre, en traversant potentiellement un ensemble de réseaux locaux hétérogènes, sans offrir aucune qualité de service ni de sécurité dans sa version intiale. Cependant, le protocole IPSec (IP Sécurisée) permet d'introduire des mécanismes de sécurité dans la couche réseau. Le rôle de ce protocole est de garantir l'`intégrité`, l'`authenticité` et la `confidentialité` des datagrammes qui sont véhiculés. IPsec peut, soit relier 2 entités communicant de bout en bout, soit relier 2 passerelles afin d'assurer les propriétés de sécurité entre deux réseaux d'entreprise reliés par ces passerelles.

Dans le cas des équipements grand public connectés à Internet, on ne peut supposer qu'ils soient reliés d'une façon ou d'une autre à une passerelle qui implémente IPSEC. Il est donc nécessaire d'envisager un déploiement dans l'équipement lui-même. Ceci nécessite donc que l'implémentation et la configuration d'IPSEC soit embarquée dès la conception de l'équipement par le fabricant. Cependant, la configuration d'IPsec reste lourde, et demande un investissement important. C'est pourquoi, il semble peu probable de voir rapidement un tel mécanisme sur des équipements grand public connectés à Internet. Un autre argument vient conforter ce sentiment. IPsec est intégré nativement dans IPv6 (alors qu'il nécessite l'application d'un patch dans IPv4), et on constate aujourd'hui que le déploiement de ce dernier est très lent. Une des raisons à la lenteur de son déploiement sur la planète est notamment la difficulté de configuration de la partie IPsec. Par conséquent, là où IPv6 est déployé aujourd'hui, très souvent la couche IPsec est désactivée. Ceci nous apporte un argument supplémentaire en faveur d'une faible probabilité de le voir un jour intégré à des équipements grand public.

5.3.3 Les couches basses

Comme annoncé précédemment, les couches basses peuvent varier sur chaque tronçon du canal de communication. Dans le cadre de cette thèse, nous nous intéressons principalement aux communications sortant du domicile, c'est pourquoi, nous nous intéressons dans cette sous-section à la pile de protocoles généralement mise en œuvre dans le cadre de connexions Internet grand public de type ADSL.

5.3.3.1 La couche liaison

PPP

La couche PPP est massivement utilisée pour les connexions à Internet grand public car elle permet d'agréger plusieurs liens. En effet, essentiellement dans les zones rurales, les équipements d'accès au réseau Internet sont partagés entre les

différents opérateurs. Dans ce cas, l'utilisation d'une couche PPP permet d'authentifier le client grâce à des identifiants, et de donner accès au réseau du bon fournisseur d'accès. Cependant, cette couche permet uniquement l'authentification du client sur la boucle locale vis-à-vis de son FAI. Elle n'assure en aucun cas la confidentialité et l'intégrité des données échangées. Elle ne permet pas non plus de vérifier l'authenticité de l'UAI vis-a-vis du DSLAM et réciproquement.

AAL & ATM

Alors que nous n'avons constaté aucun mécanisme de sécurité au niveau ATM lors de nos travaux, il existe, depuis de nombreuses années, un ensemble d'approches pour la sécurité des communications ATM [68]. Ces approches se divisent suivant que la négociation du contexte de sécurité :

— modifie la phase de négociation, en y ajoutant des informations de sécurité.
— modifie les flux de gestion, en y introduisant des informations de sécurité, en continu.
— injecte des données utilisateurs contenant les informations de sécurité avant l'envoi des données de la communication.

Dans tous les cas, les différentes approches permettent, à l'aide des informations de sécurité (clefs de chiffrement, certificats, etc.) d'assurer les trois propriétés usuelles de sécurité, plus une protection contre les tentatives d'analyses statistiques au moyen d'un mécanisme de `bourrage` [1].

Cependant, ces mécanismes de sécurité permettent uniquement de sécuriser le tronçon du réseau fondé sur une couche ATM. De plus, le partage des équipements terminaux (DSLAM) entre les différents FAI [2] nécessiterait une entente globale sur les approches à adopter, ce qui paraît aujourd'hui difficilement réalisable.

5.3.3.2 La couche physique

La majorité des supports physiques, comme la paire de cuivre par exemple, nécessitent la connaissance de la longueur du canal de communication afin de négocier [11] le débit atteignable sur celui-ci. Cette valeur devrait drastiquement varier lorsqu'une plateforme telle que celle utilisée pour observer les communications des UAI, est insérée sur la boucle locale. Ce principe est illustré dans la Figure 5.5.

L'une des deux entités pourrait alors émettre une alerte informant l'utilisateur ou le fournisseur de service d'une situation anormale et l'inciter à être vigilant. Ce cas est d'autant plus pertinent que les connexions filaires ne sont que rarement remplacées. De plus, la surveillance de cette mesure permettrait de détecter de manière générale toute interruption d'une ligne et d'optimiser les opérations de maintenance. Toutefois, cette mesure permet simplement d'effectuer de la détection d'attaque et ne permet en aucun cas de s'en prémunir.

1. Génération de trafic supplémentaire, non significatif, afin d'éviter toute tentative d'analyse statistique des données.
2. Sauf en cas de dégroupage total.

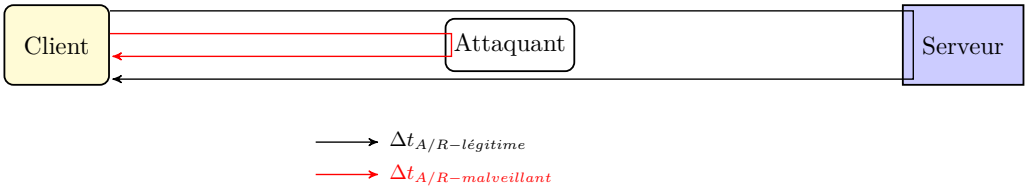


FIGURE 5.5 – Calcul du temps aller/retour

5.3.4 Synthèse

Nous venons d'aborder différents mécanismes de sécurité applicables pour chaque couche protocolaire d'une connexion Internet grand public. Alors qu'il semble difficile de sécuriser les couches basses, à cause de leur hétérogénéité éventuelle et le coût de déploiement que cela nécessiterait, plusieurs mécanismes de sécurité robustes existent pour les couches hautes. Nous recommandons l'usage systématique des mécanismes de sécurité au niveau applicatif et au niveau transport. Au niveau applicatif, nous conseillons, si possible, l'utilisation de librairies existantes reconnues robustes. Au niveau transport nous conseillons, si possible, la mise en œuvre d'une couche TLS.

Cependant, nous insistons sur l'importance de correctement implémenter, configurer et maintenir à jour ces mécanismes. En effet, de nombreuses failles de sécurité sont dues à une mauvaise implémentation ou à une absence de mise à jour de TLS.

5.4 La connexion au réseau télévisuel hertzien

Notre deuxième cas d'étude, concernant la sécurité des téléviseurs connectés à Internet, nous a conduit à étudier la sécurité des flux télévisuels hertziens. Les différentes expérimentations que nous avons menées nous ont permis de mettre en évidence un certain nombre de failles de sécurité pour lesquelles il existe différents mécanismes de sécurité. Dans cette section, nous présentons dans un premier temps la pile de protocole d'une émission de télévision hertzien, puis, dans un second temps, les différentes contre-mesures aux problèmes de sécurité identifiés.

5.4.1 Pile de protocoles

La majorité des moyens de réception de la télévision fonctionnent sur le principe d'une communication unidirectionnelle. Comme l'émission de flux hertziens, sur la bande de fréquence réservée à la télévision, est interdite sans licence dans la plupart des pays, la définition des protocoles utilisés est moins détaillée. Cependant, l'expérience acquise lors des travaux réalisés dans le cadre de cette thèse met en évidence les trois couches représentées dans la Figure 5.6.

№	№ OSI	Nom	Description
3	5-7	Application	Flux élémentaires multimédia & données
2	4	Transport	Multiplexage DVB
1	1-3	Physique	Définition des paramètres de transmission physique

FIGURE 5.6 – Pile DVB

5.4.2 Les couches hautes

Les couches hautes d'une émission télévisuelle suivant la norme DVB sont indépendantes du support de transmission utilisé. Les mécanismes de sécurité s'appliquant à ces couches sont donc valables, quelle que soit la forme de DVB (DVB-S, DVB-C ou DVB-T) utilisée.

5.4.2.1 La couche application

La couche applicative des émissions DVB représente les différents protocoles utilisés par les différents flux élémentaires d'une émission hertzienne. On y retrouve les flux Video et Audio au format MPEG-2 ainsi que des flux de données. Si des mécanismes de sécurité [31, 32] pour MPEG existent, ils sont généralement orientés vers la protection des droits d'auteur (DRM), mais ne permettent en aucun cas au téléspectateur de s'assurer de l'intégrité ou de l'authenticité du flux.

5.4.2.2 La couche transport

La couche transport des émissions DVB représente le multiplexage des différents flux élémentaires dans un multiplex MPEG-TS. Afin de permettre la diffusion de chaînes payantes, DVB utilise le *Common Scrambling Algorithm* (CSA). Ce mécanisme permet, à l'aide d'un système de chiffrement symétrique, d'offrir un système de contrôle d'accès aux opérateurs TV pour le contenu payant.

La clef de chiffrement est transmise à l'intérieur du flux avec le contenu chiffré, protégé par un système de chiffrement asymétrique. Le téléspectateur possède une carte à puce, capable de déchiffrer la clef de chiffrement, afin de déchiffrer ensuite le contenu télévisuel. Ce mécanisme est uniquement destiné à un contrôle d'accès mais ne permet pas par exemple d'authentifier l'emetteur DVB, ni l'origine des données reçues.

En résumé, les protocoles utilisés sur les couches hautes d'une transmission télévisuelle ne permettent pas d'assurer l'`intégrité` des méta-données du flux et donc d'assurer son `authenticité`. Pour cela il serait nécessaire d'implémenter, par exemple, un système permettant de vérifier un certificat émis par l'opérateur TV. Ceci nécessiterait la mise en place d'une infrastructure de clefs publiques, d'autorité de certification associée afin de déployer des certificats et de pouvoir les vérifier.

5.4.3 Les couches basses

Les couches basses d'une émission télévisuelle suivant la norme DVB dépendent du support de transmission utilisé. Cependant, les trois principaux supports de communication utilisés ont un point commun qui peut être validé sur chaque support avec un équipement analogue. En effet, pour une émission DVB-T, utilisée pour la télévision numérique terrestre, nous rappelons que des seuils sont officiellement définis par L'Union Internationale des Télécommunications [60], de façon à ce qu'un signal plus faible ne puisse interférer avec un signal plus fort. Ceci implique que, pour qu'une attaque puisse fonctionner, l'entité réceptrice doit implicitement recevoir un signal plus puissant pendant la durée de l'attaque. Cette situation est présentée dans la Figure 5.7.

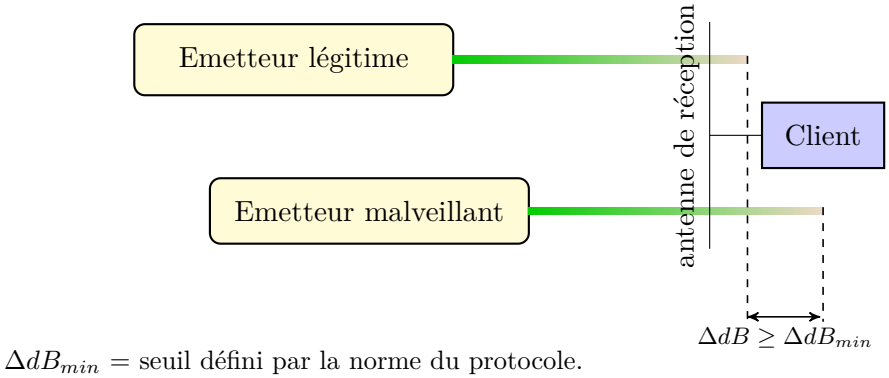


FIGURE 5.7 – Écart de puissance du signal reçu

L'entité réceptrice, le téléviseur en l'occurrence, pourrait alors informer l'utilisateur d'une situation anormale et l'inciter à être vigilant vis-à-vis des informations affichées sur son téléviseur. Notons que ce mécanisme, contrairement à celui décrit pour les connections filaires (cf. section 5.3.3.2), ne s'applique pas à tous les types de connexion sans-fil. En effet, il est pertinent dans le cadre des émissions TV, où l'entité émettrice ne bouge jamais, et l'entité réceptrice rarement. Dans ce cas, la puissance du signal ne varie jamais ou alors très légèrement. Cependant, pour d'autres types de communications, comme la téléphonie GSM, où l'entité réceptrice est toujours en mouvement, ce concept ne serait pas pertinent.

Par ailleurs, les chaînes TV se soucient de la qualité de service fourni aux téléspectateurs. C'est pourquoi, les opérateurs TV déploient des "vérificateurs" [53] à différents endroits du territoire. Ces vérificateurs sont capables de comparer le signal reçu au signal émis par l'antenne TV. Les principales missions de ces vérificateurs consistent à :

— Vérifier la qualité du signal sur le territoire.
— Vérifier l'intégrité du signal : *Est-ce que sur la fréquence de France 2, on reçoit bien le signal correspondant à France 2 ?*
— Vérifier l'authenticité du signal : *Est-ce que le signal sur la fréquence de*

France 2 provient bien de l'antenne destinée à émettre ce signal ?

— Détecter d'éventuelles émissions pirates.

Malheureusement nous n'avons que peu d'informations concernant les méthodes employées par ces vérificateurs, gardées secrètes afin d'éviter toute tentative de contournement de celles-ci. Cependant, nous savons qu'une comparaison avec une autre source est effectuée, probablement via un lien Internet, et que des marqueurs sont injectés dans le signal d'origine. La sécurité que peut apporter ce mécanisme réside dans le fait qu'il est facilement possible ou non de contrefaire les marqueurs mais nous ne disposons malheureusement pas des informations permettant d'en juger. S'ils sont effectivement impossibles à contrefaire, alors, ce mécanisme est très intéressant du point de vue de la sécurité car il permet de garantir l'authenticité d'un signal et il permet donc à un utilisateur d'être certain que le signal qu'il reçoit a bien été émis par l'émetteur légitime.

5.4.4 Synthèse

D'un point de vue de la sécurité de l'information, nous considérons qu'il est primordial de faire évoluer les standards DVB afin d'intégrer obligatoirement un système de vérification de certificat lors de transferts de code informatique à l'intérieur d'un flux DVB. Ce mécanisme serait semblable au fonctionnement d'un navigateur Internet. Ainsi, seules les données signées par un certificat reconnu par le téléviseur pourront s'exécuter sur celui-ci. Par extension, ce concept pourrait être étendue en joignant régulièrement, par exemple, une somme de contrôle de tous les flux du multiplex, signée par l'émetteur.

5.5 Conclusion

Dans ce chapitre, nous avons abordé la problématique générale soulevée à travers les deux cas d'études présentés dans les chapitres 3 et 4. Nous avons étudié les deux piles de protocoles mises en œuvre, afin d'analyser les mécanismes de sécurité adaptés à chaque couche. Certaines de ces contre-mesures sont redondantes, mais se situent à des niveaux protocolaires différents. Ainsi, en cas de défaillance de l'un de ces mécanismes, la sécurité globale peut quand même être assurée, tant que d'autres mécanismes situés à d'autres niveaux sont opérationnels.

La principale problématique restante est de savoir qui prend en charge le déploiement de ces différents mécanismes de sécurité. En considérant que l'utilisateur moyen n'a pas les compétences nécessaires pour modifier les applications contenues dans un équipement grand public connecté à Internet, cette tâche revient automatiquement au fabricant. Toutefois, certaines contre-mesures nécessitent des investissements plus lourds que d'autres, ou sont plus gourmandes en terme de puissance de calcul nécessaire. C'est pourquoi il est primordial de prendre en compte la sécurité d'un équipement dès de sa conception.

En ce qui concerne les connexions à l'Internet grand public, la mise en place systématique de méthodes de chiffrement telles que TLS est réalisable sans inves-

tissements importants. En revanche, pour les émissions télévisuelles hertziennes, il n'existe, à notre connaissance, pas de mécanisme permettant de sécuriser correctement les téléviseurs connectés. Une évolution de la norme serait la solution idéale face aux problèmes identifiés.

Conclusion générale

Bilan

La sécurité informatique ainsi que le respect de la vie privée sont devenus, au fil des années, des préoccupations centrales, tant pour le secteur de l'industrie que pour le monde académique. Toutefois, alors que la sécurité des équipements et des infrastructures industrielles est à l'étude depuis déjà de nombreuses années, la sécurité des équipements grand public est encore aujourd'hui relativement peu étudiée. Le but de cette thèse était donc de contribuer à l'analyse de la sécurité de ces matériels.

Dans ce manuscrit, nous avons présenté une méthode applicable à tout équipement grand public connecté à Internet, destinée à analyser la sécurité de ses liens de communication. En effet, avec l'arrivée de l'"Internet des Objets" et la tendance au "tout connecté", le nombre d'équipements grand public connectés à Internet est en croissance constante. Afin de montrer la pertinence de cette méthode, nous l'avons appliquée à deux cas d'étude, présentés dans les chapitres 3 et 4.

La première phase de l'approche que nous avons proposée repose sur des méthodes éprouvées, issus du monde industriel. Il s'agit des méthodes d'analyse des risques des systèmes d'information. La richesse de ces méthodes permet d'étudier les risques de tout système d'information et les équipements grand public connectés à Internet en font partie. Cette première phase permet d'identifier et de prioriser les risques ciblant l'équipement étudié. La seconde phase de notre méthode concerne la validation technique des scénarios menant aux risques identifiés lors de la première phase. Nous avons proposé d'établir cette validation technique en trois sous-étapes. Cette seconde phase est ainsi composée :

— une observation passive du lien de communication concerné ;
— une simulation de l'environnement qui communique avec l'équipement sur ce lien ;
— de tentatives d'attaque.

Dans le cadre de deux cas d'étude, cette méthode nous a permis d'identifier et de valider techniquement plusieurs failles de sécurité, pour les téléviseurs connectés et les unités d'accès intégrées, pour lesquels il y a peu de résultats publiés sur leur sécurité.

Avant de conclure ce manuscrit, nous avons présenté les différentes contremesures que nous pouvons proposer face aux failles de sécurité découvertes durant ces travaux.

Perspectives

Une première perspective immédiate découlant de ces travaux est bien sûr la généralisation à d'autres équipements grand public du même type. En ce sens, nous

pensons qu'il serait nécessaire d'envisager ce type d'études pour tous les équipements grand public disponibles sur le marché. Étant donné la difficulté pour un utilisateur quelconque de s'assurer de la sécurité d'un équipement qu'il connecte à son réseau informatique, nous pensons qu'il serait important de mener systématiquement ce genre d'évaluation sur tout matériel grand public connecté (par des centres d'évaluation officiels par exemple) afin de pouvoir leur attribuer une classification normalisée et reconnue, permettant de représenter le niveau de sécurité de l'équipement. Une telle classification pourrait consister à associer un niveau de sécurité à chaque équipement, comme cela est le cas aujourd'hui pour la consommation électrique de certains appareils par exemple. Ainsi, il est possible que, sensibilisé par la sécurité et le respect de sa vie privée, l'utilisateur puisse préférer acquérir un équipement certifié à un niveau de sécurité élevé, plutôt qu'un autre équipement moins bien noté. Instaurer ce type de certification aurait un double avantage :

— informer l'utilisateur et le sensibiliser aux risques liés aux problèmes de sécurité informatique lorsqu'il achète un équipement (risques que souvent il ignore, au moins en partie) ;
— inciter les fabricants à intégrer la sécurité au plus tôt (dès la conception) dans le processus de développement de leurs produits.

Une autre perspective à ces travaux concerne l'étude globale de la sécurité du domicile connecté. De la même façon que nous l'avons menée dans cette thèse sur des matériels spécifiques, il convient aujourd'hui, de réaliser une analyse des risques sur l'ensemble du réseau domestique avec ses différents équipements connectés. En effet, nos travaux ont permis de révéler plusieurs failles de sécurité intéressantes, dont certaines mettent en jeu plusieurs équipements à la fois. Dans une vision globale des systèmes d'information domestiques, il est essentiel de définir des règles génériques en ce qui concerne les équipements grand public connectés à Internet. Une telle étude pourrait amener à l'élaboration de règles et principes de sécurité applicables, comme par exemple :

— Tous les équipements connectés à l'intérieur du domicile doivent être considérés comme une source potentielle de menaces.
— Les équipements "nomades" ne doivent pas avoir le même statut de sécurité que les équipements résidents, dans la mesure où le risque de compromission est plus élevé.
— Toute entité extérieure au domicile ne doit pas avoir accès à plus d'informations que celles qui lui sont envoyées de manière légitime.
— Tout accès privilégié depuis l'extérieur du réseau domestique doit être authentifié.

Il serait important que de telles règles de sécurité, relatives à la sécurité du domicile connecté, existent et soient systématiquement appliquées lors de l'ajout d'un nouvel équipement au sein du domicile. Bien évidemment, les quelques règles énoncées ci-dessus ne sont que des exemples mais il nous semble fondamental de tendre à une élaboration précise et la plus exhaustive possible de règles de ce type afin de contribuer à l'amélioration de la sécurité du domicile connecté.

Dans le dernier chapitre de cette thèse, nous avons abordé concrètement différents mécanismes de sécurité, permettant d'améliorer la sécurité des équipements grand public connectés à Internet. La majorité de ces mécanismes existent déjà, et peuvent généralement être intégrés assez facilement par le fabricant. Dans certains cas, comme pour les téléviseurs connectés par exemple, alors que les mécanismes de sécurité existent, leur implémentation n'est pas prévue dans le protocole de communication. Pour cela, il est a priori nécessaire de revoir les normes en vigueur afin d'y inclure les mécanismes de sécurité appropriés. L'étude systématique des normes et standards utilisés dans le cadre de tous les protocoles de communication, utilisés par ces équipements, quel que soit leur support, de façon à y intégrer des mécanismes de sécurité, nous semble ainsi constituer une perspective intéressante et utile à nos travaux.

Alors que les équipements étudiés dans ce manuscrit sont capables d'intégrer des mécanismes de sécurité semblables à ceux habituellement utilisés par les systèmes informatiques, ceci n'est a priori pas le cas pour tous les équipements connectés. En effet, dans le premier chapitre de ce manuscrit, nous avons distingué les objets connectés des objets communicants. Ces objets communicants sont souvent de petits capteurs, uniquement capables de communiquer l'état de l'objet sur lequel ils sont placés. Afin de réduire le coût de fabrication de ces capteurs, ils n'intègrent généralement que très peu de ressources de calcul et leur autonomie énergétique est souvent très limitée. C'est pourquoi il n'est généralement pas possible d'intégrer des mécanismes lourds, cryptographiques par exemple, dans ce type d'objets. Une étude sur les mesures de sécurité applicables dans le cadre de ces micro-capteurs et de tous les objets connectés de façon générale, en fonction de leurs différentes caractéristiques (matérielles et logicielles) constitue selon nous une autre perspective pertinente à nos travaux.

Le problème de la protection de la vie privée n'a pas été abordé exhaustivement dans cette thèse et il constitue une étude qu'il est aujourd'hui incontournable de mener. Dans la section 5.3.2.1, nous avons présenté un concept permettant à un utilisateur d'anonymiser, de manière indépendante de l'équipement, les données sortant de son domicile sur sa connexion Internet. D'une manière plus générale, il nous semble nécessaire d'imaginer des méthodes et outils permettant ce type de contrôle et/ou d'anonymisation des données pouvant sortir du domicile. Par exemple, on peut imaginer un équipement capable d'analyser tous les flux sortant sur le lien Internet du domicile, quels que soient les équipements utilisés par l'utilisateur. Cet équipement permettrait, à l'aide d'une interface utilisateur, d'identifier tous ces flux et de les associer aux équipements connectés au réseau informatique du domicile. Relié au pare-feu et à une plateforme collaborative, l'utilisateur pourrait ainsi choisir de bloquer purement et simplement un flux, le mélanger à des profils d'utilisation d'autres utilisateurs ou bien de le rediriger à travers des réseaux destinés à anonymiser les données, comme celui du projet "Tor" (*The Onion Router*) [42] par exemple.

Enfin, dans cette thèse, nous avons privilégié l'étude des moyens de communication relatifs aux équipements grand public connectés à Internet. Cependant, d'autres

surfaces d'attaque existent, et méritent d'être étudiées. En effet, outre ses différentes connectivités, un objet connecté contient des applications, un système d'exploitation, des protocoles de communication ou encore une architecture matérielle (parfois propriétaire) éventuellement non sécurisée. Tous ces objets complexifient le système d'information global présent dans les domiciles. Ainsi, inévitablement, des moyens de protection contre les malveillances suffisamment efficaces devront être déployés pour les systèmes d'information grand public.

Bibliographie

[1] Open freebox : Cette box se devait d'etre ouverte, libre et gratuite... http://www.f-x.fr/. (visité le 2015-04-28). (Cité en page 23.)

[2] Openbox4 : Modifier et personnaliser la box de sfr. http://www.neufbox4.org. (visité le 2015-04-28). (Cité en page 23.)

[3] Openlgtv. http://openlgtv.org.ru/wiki/index.php/Wiki_index. (visité le 2015-04-28). (Cité en page 23.)

[4] A. Adelsbach, C. Cachin, S. Creese, Y. Deswarte, K. Kursawe, J-C. Laprie, D. Powell, B. Randell, J. Riodan, P. Ryan, et al. Conceptual model and architecture of maftia. 2003. (Cité en pages 7, 8 et 10.)

[5] Agence nationale de la sécurité des systèmes d'information (ANSSI). Expression des besoins et identification des objectifs de sécurité. http://www.ssi.gouv.fr/entreprise/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/, 2010. (visité le 2015-04-28). (Cité en page 39.)

[6] Agence nationale de la sécurité des systèmes d'information (ANSSI). Méthodologie pour l'évaluation logicielle des terminaux de réception numérique en vue d'une certification de sécurité de premier niveau. http://www.ssi.gouv.fr/uploads/2015/01/ANSSI-CSPN-NOTE-02_Methodologie_pour_evaluation_CSPN_de_STB_v1-0.pdf, 2014. (visité le 2015-04-28). (Cité en page 27.)

[7] E. U. Altinyurt. Samygo. http://www.samygo.tv. (visité le 2015-04-28). (Cité en page 23.)

[8] T. W. Anderson and P. A. Lee. *Fault tolerance : principles and practice*. Prentice-Hall, Englewood Cliffs, NJ, 1981. (Cité en page 8.)

[9] O. Antolinez. La web 2.0 - definición. https://web.archive.org/web/20070928013821/http://www.oscarantolinez.com/2007/07/27/la-web-20-definicion/, 2007. (archive visitée le 2015-04-28). (Cité en page 11.)

[10] J. Arlat, J.-P. Blanquart, A. Costes, Y. Crouzet, Y. Deswarte, J.-C. Fabre, H. Guillermain, M. Kâaniche, K. Kanoun, J.-C. Laprie, C. Mazet, D. Powell, C. Rabéjac, and P. Thévenod. *Guide de la sûreté de fonctionnement*. Cépaduès-éditions, 1996. (Cité en page 6.)

[11] Autorité de régulation des communications électroniques et des postes (ARCEP). Avis du Comité d'Experts concernant l'autorisation de la technique READSL2 au répartiteur dans le cadre de l'accès à la boucle locale de France Télécom. http://www.arcep.fr/fileadmin/reprise/dossiers/internet/avis-fin-readsl2.pdf, 2005. (visité le 2015-04-28). (Cité en page 105.)

[12] Autorité de régulation des communications électroniques et des postes (ARCEP). Observatoire trimestriel des marchés de détail des communications électroniques (services fixes haut et très haut débit) en France - 3e trimestre 2013. `http://www.arcep.fr/index.php?id=12747`, 2013. (visité le 2015-04-28). (Cité en page 58.)

[13] Autorité de régulation des communications électroniques et des postes (ARCEP). Les brouilleurs et répéteurs de réseaux mobiles. `http://arcep.fr/index.php?id=11946`, 2014. (visité le 2015-04-28). (Cité en page 26.)

[14] A. Avižienis. Design of fault-tolerant computers. In *Proceedings of the November 14-16, 1967, Fall Joint Computer Conference*, AFIPS '67, pages 733–743, New York, NY, USA. ACM. (Cité en page 8.)

[15] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaâniche, J-C. Courrège, and P. Lukjanenko. Smart-tv security analysis : practical experiments. In *Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages –8, Jun 2015. (Cité en page 77.)

[16] Y. Bachy, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and J-C. Courrège. Analyse de sécurité des box adsl. In *Symposium sur la sécurité des technologies de l'information et des communications*, pages –15, Jun 2014. (Cité en page 60.)

[17] Y. Bachy, V. Nicomette, E. Alata, M. Kaâniche, and J-C. Courrège. La sécurité des box adsl : analyse de risques et éxpériementations. *Ingénierie des systèmes d'information*, 19(6) :63–88, Nov 2014. (Cité en page 48.)

[18] Y. Bachy, V. Nicomette, E. Alata, M. Kaâniche, and J-C. Courrège. Security of isp access networks : practical experiments. In *11th European Dependable Computing Conference - Dependability in Practice*, Sep 2015. (Cité en page 59.)

[19] Y. Bachy, V. Nicomette, E. Alata, M. Kaâniche, J-C. Courrège, and P. Lukjanenko. Protocole hbbtv et sécurité : quelques expérimentations. In *Symposium sur la sécurité des technologies de l'information et des communications*, pages –13, Jun 2015. (Cité en page 77.)

[20] F. Basse. Sécurité des ordivisions. In *proc. of Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, Rennes, France, juin 2014. (Cité en pages 23, 24 et 84.)

[21] F. Basse. Télévisions connectées : Des objets branchés sécurité ? *Multi-System and Internet Security Cookbook (MISC)*, September / October 2014. (Cité en pages 23, 24 et 84.)

[22] P-J. Benghozi, S. Bureau, F. Massit-Folléa, C. Waroquiers, and S. Davidson. *L'internet des objets : quels enjeux pour l'Europe*. Éd. de la Maison des sciences de l'homme, 2009. (Cité en page 12.)

[23] T. Berners-Lee, J. Hendler, O. Lassila, et al. The semantic web. *Scientific american*, 284(5) :28–37, 2001. (Cité en page 12.)

[24] A. Bittau, M. Handley, and J. Lackey. The final nail in wep's coffin. In *Security and Privacy, 2006 IEEE Symposium on*, pages 15 pp.–400, May 2006. (Cité en page 26.)

[25] Bogdan. Dvb-t implementation in gnuradio ? part 2. `http://yo3iiu.ro/blog/?p=1220`. (visité le 2015-04-28). (Cité en page 77.)

[26] H. Bojinov, E. Bursztein, and D. Boneh. XCS : Cross Channel Scripting and Its Impact on Web Applications. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 420–431, New York, NY, USA, 2009. ACM. (Cité en page 24.)

[27] C. Botnet. Port scanning /0 using insecure embedded devices. `http://internetcensus2012.bitbucket.org/paper.html`, 2012. (visité le 2015-04-28). (Cité en page 21.)

[28] S. Bushell. M-commerce key to ubiquitous Internet. `http://www.computerworld.com.au/article/84178/m-commerce_key_ubiquitous_internet/`, 2000. (visité le 2015-04-28). (Cité en page 12.)

[29] Instituts Carnot. *Objets communicants et Internet des objets*. 2011. (Cité en page 12.)

[30] CERT. Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. `http://www.cert.org/downloads/octave-allegro/OCTAVE-AllegroMethod-v10.pdf`, 2007. (visité le 2015-04-28). (Cité en page 39.)

[31] F. Chen-Wei, C. Feng-Cheng, and H. Hsueh-Ming. An MPEG-4 IPMPX design and implementation on MPEG-21 test bed. In *International Symposium on Circuits and Systems, 2005. ISCAS 2005.*, pages 4550–4553 Vol. 5, May 2005. (Cité en page 107.)

[32] Y. Cho, J. Seok, J. Hong, and C. Ahn. Broadcasting system compliant with MPEG-2/4 IPMPX. *Electronics and Telecommunications Research Institute journal (ETRI)*, 26(2) :83–91, 2004. (Cité en page 107.)

[33] CLUSIF. Méthode harmonisée d'analyse des risques. `https://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principes-Specifications.pdf`, 2010. (visité le 2015-04-28). (Cité en page 37.)

[34] European Commission. Special eurobarometer 396 - e-communications household survey. `http://ec.europa.eu/digital-agenda/en/news/special-eurobarometer-396-e-communications-household-survey`, 2013. (visité le 2015-04-28). (Cité en page 76.)

[35] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. A large scale analysis of the security of embedded firmwares. *USENIX Security. USENIX Association*, 2014. (Cité en page 21.)

[36] D. Crockford. *JavaScript : The Good Parts*. O'Reilly Media, Inc., 2008. (Cité en page 81.)

[37] CSMAU. Réfrigérateur intelligent avec lecteur RFID vous alerte lorsque vous êtes à court de stock. `http://www.csmau.com/refrigerateur-intelligent-avec-lecteur-rfid-vous-alerte-lorsque-vous-etes-a-court-de-stock.html`. (visité le 2015-04-28). (Cité en page 14.)

[38] A. Cui, Y. Song, P. V. Prabhu, and S. J. Stolfo. Brave new world : Pervasive insecurity of embedded network devices. In Engin Kirda, Somesh Jha, and Davide Balzarotti, editors, *Recent Advances in Intrusion Detection*, volume 5758 of *Lecture Notes in Computer Science*, pages 378–380. Springer Berlin Heidelberg, 2009. (Cité en pages 21 et 27.)

[39] A. Cui and S. J. Stolfo. A quantitative analysis of the insecurity of embedded network devices : Results of a wide-area scan. In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pages 97–106, New York, NY, USA, 2010. ACM. (Cité en page 21.)

[40] J. Daemen and V. Rijmen. *The design of Rijndael : AES-the advanced encryption standard*. Springer Science & Business Media, 2002. (Cité en page 23.)

[41] Y. Deswarte. *La sécurité des systèmes d'information et de communication*. Traité IC2, Hermès, 2006. (Cité en page 9.)

[42] R. Dingledine, N. Mathewson, and P. Syverson. Tor : The second-generation onion router. Technical report, DTIC Document, 2004. (Cité en page 113.)

[43] 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. (visité le 2015-04-28). (Cité en pages 90 et 91.)

[44] C. Douligeris and A. Mitrokotsa. DDoS attacks and defense mechanisms : classification and state-of-the-art. *Computer Networks*, 44(5) :643 – 666, 2004. (Cité en page 25.)

[45] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, and V. Paxson. The matter of heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, IMC '14, pages 475–488, New York, NY, USA, 2014. ACM. (Cité en page 103.)

[46] K. Egevang and P. Francis. The ip network address translator (nat). `http://www.hjp.at/doc/rfc/rfc1631.html`, 1994. (visité le 2015-05-05). (Cité en page 20.)

[47] M. Eoloff, J. Egasti, J. Krall, and K. Kosobucki. The smart fridge. `http://www.mu.edu/~owt/SmartFridge.pdf`. (visité le 2015-04-28). (Cité en page 14.)

[48] European Broadcasting Union. *ETSI TS 102 796 V1.2.1*. November 2012. (Cité en pages 79 et 82.)

[49] Commission européenne. Stratégie numérique : la Commission lance une consultation sur les règles concernant les dispositifs connectés intelligents -

l'"internet des objets". http://europa.eu/rapid/press-release_IP-12-360_fr.htm, 2012. (visité le 2015-04-28). (Cité en page 93.)

[50] Independent Security Evaluators. SOHO Network Equipment and the implications of a rich service set. https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf, 2013. (visité le 2015-04-28). (Cité en pages 17 et 21.)

[51] A. Fernandez-Toro. *Management de la sécurité de l'information : Implémentation ISO 27001 - Mise en place d'un SMSI et audit de certification*. Solutions d'entreprise. Eyrolles, 2009. (Cité en page 35.)

[52] J. Firmage. Newsmaker : Portals in space. https://web.archive.org/web/20081119064424/http://www.news.com/2008-1082_3-5056441.html, 2003. (archive visitée le 2015-04-28). (Cité en page 11.)

[53] W. Fischer. Measurements on the MPEG-2 Transport Stream. In *Digital Video and Audio Broadcasting Technology*, Signals and Communication Technology, pages 179–195. Springer Berlin Heidelberg, 2008. (Cité en page 108.)

[54] P. Gautier. Web 3.0, web sémantique, internet des objets. http://david.fayon.free.fr/interview/philippe-gautier.htm, 2010. (visité le 2015-04-28). (Cité en page 11.)

[55] M. Ghiglieri and E. Tews. A privacy protection system for HbbTV in Smart-TVs. In *11th Consumer Communications and Networking Conference (CCNC)*, pages 357–362, Jan 2014. (Cité en page 26.)

[56] T. Goodspeed. Emulating USB DFU to Capture Firmware. http://travisgoodspeed.blogspot.com/2012/10/emulating-usb-dfu-to-capture-firmware.html, 2012. (visité le 2015-04-28). (Cité en page 24.)

[57] M. Harris Cheheyl, M. Gasser, G. A. Huff, and J. K. Millen. Verifying security. *ACM Computer Survey*, 13(3) :279–339, September 1981. (Cité en page 8.)

[58] C. Heffner. Reverse Engineering a D-Link Backdoor. http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/, 2013. (visité le 2015-04-28). (Cité en page 25.)

[59] IEEE. IEEE Standard Glossary of Software Engineering Terminology. *IEEE Std 610.12-1990*, pages 1–84, Dec 1990. (Cité en page 16.)

[60] International Telecommunication Union. Planning criteria, including protection ratios, for digital terrestrial television services in the vhf/uhf bands, 2014. (Cité en pages 78 et 108.)

[61] ISO. ISO 31000 - Management du risque. http://www.iso.org/iso/fr/home/standards/iso31000.htm, 2013. (visité le 2015-04-28). (Cité en page 33.)

[62] M. Jordon. Hacking Canon Pixma Printers - Doomed Encryption. http://www.contextis.co.uk/resources/blog/hacking-canon-pixma-printers-doomed-encryption/, 2014. (visité le 2015-04-28). (Cité en page 25.)

[63] M. Kenney. Ping of Death. `http://insecure.org/sploits/ping-o-death.html`, 1996. (visité le 2015-04-28). (Cité en page 25.)

[64] Kingcope, M. Fujiwara, and M. Neis. Apache Range Header DoS (Apache Killer). `https://web.archive.org/web/20130924235327/http://www.rapid7.com/db/modules/auxiliary/dos/http/apache_range_dos`, 2011. (archive visitée le 2015-04-28). (Cité en page 25.)

[65] Kolibree. La brosse à dents Kolibree, le compagnon efficace et agréable d'une bonne hygiène dentaire pour toute la famille. `http://www.kolibree.com/fr/product/`. (visité le 2015-05-05). (Cité en page 13.)

[66] R. Kuipers, E. Starck, and H. Heikkinen. Smart tv hacking : Crash testing your home entertainment. *Codenomicon Whitepaper*, 2012. (Cité en page 21.)

[67] La Commission Nationale de l'Informatique et des Libertés. Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-ii de la loi du 6 janvier 1978. `http://www.cnil.fr/documentation/deliberations/deliberation/delib/300/`, 2013. (visité le 2015-04-28). (Cité en page 92.)

[68] M. Laurent and P. Rolin. Etat de l'art de la securité sur ATM. *De Nouvelles Architectures pour les Communications (DNAC'96)*, pages 323–341, 1996. (Cité en page 105.)

[69] Le bon plan. Des décodeurs pirates (DreamBox, Samsat) pour regarder Canal+, CanalSat, BeinSport. `http://www.le-bon-plan.com/decodeurs-pirates-dreambox-samsat-regarder-canal-canalsat-beinsport.html`, 2014. (visité le 2015-04-28). (Cité en page 24.)

[70] E. le Ricque. Brouilleur de téléphone, le gadget interdit. `http://www.tomsguide.fr/article/brouilleur-ondes-3G-GSM-smartphone,2-896.html`, 2013. (visité le 2015-04-28). (Cité en page 26.)

[71] O. Levillain. SSL/TLS : état des lieux et recommandations. In *proc. of Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, Rennes, France, June 6th 2012. (Cité en pages 63 et 102.)

[72] K. Lovett. Full Disclosure ASUS Wireless Routers Ten Models - Multiple Vulnerabilities on AiCloud enabled units. `http://www.securityfocus.com/archive/1/527275/30/0/threaded`, 2013. (visité le 2015-04-28). (Cité en page 25.)

[73] J. Luczak-Rougeaux. La Sense Mother, l'appareil qui se connecte au quotidien. `http://www.tom.travel/2014/07/la-sense-mother-lappareil-qui-se-connecte-au-quotidien/`, 2014. (visité le 2015-04-28). (Cité en page 13.)

[74] A. Lupfer. *Gestion des risques en sécurité de l'information : mise en oeuvre de la norme ISO 27005*. Solutions d'entreprise. Eyrolles, 2010. (Cité en page 36.)

[75] E. Messmer. Massive DDoS attacks a growing threat to VoIP services. `http://www.networkworld.com/article/2181743/voip/massive-`

ddos-attacks-a-growing-threat-to-voip-services.html, 2011. (visité le 2015-04-28). (Cité en page 25.)

[76] U. Meyer and S. Wetzel. A Man-in-the-middle Attack on UMTS. In *Proceedings of the 3rd Workshop on Wireless Security*, WiSe '04, pages 90–97, New York, NY, USA, 2004. ACM. (Cité en page 27.)

[77] H. Moore. Security Flaws in Universal Plug and Play : Unplug. don't play. *Rapid7, Ltd.,(Jan. 2013)*, 2013. (Cité en page 21.)

[78] E. Ogez. Petite définition du Web 2.0. http://pro.01net.com/editorial/504033/petite-definition-du-web-2-0/, 2009. (visité le 2015-04-28). (Cité en page 11.)

[79] T. O'Reilly. Web 2.0 : Compact definition ? http://radar.oreilly.com/2005/10/web-20-compact-definition.html, 2005. (visité le 2015-04-28). (Cité en page 11.)

[80] T. O'Reilly. What Is Web 2.0. http://www.oreilly.com/pub/a//web2/archive/what-is-web-20.html, 2005. (visité le 2015-04-28). (Cité en page 11.)

[81] Y. Oren and A. 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. (Cité en page 82.)

[82] OWASP. Man-in-the-middle attack. https://www.owasp.org/index.php/Man-in-the-middle_attack, 2014. (visité le 2015-04-28). (Cité en page 24.)

[83] R. Paleari and A. Di Pinto. Sitecom firmware encryption and wireless keys. http://blog.emaze.net/2014/04/sitecom-firmware-and-wifi.html, 2014. (visité le 2015-04-28). (Cité en page 26.)

[84] F. Pisani. Web 3.0 : définitions. http://pisani.blog.lemonde.fr/2007/10/07/web-30-definitions/, 2007. (visité le 2015-04-28). (Cité en page 11.)

[85] J. Ruderman. The same origin policy. https://developer.mozilla.org/fr/docs/Web/JavaScript/Same_origin_policy_for_JavaScript, 2001. (visité le 2015-04-28). (Cité en page 81.)

[86] 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. (Cité en page 25.)

[87] M. Sajdak. TP-Link HTTP/TFTP backdoor. http://sekurak.pl/tp-link-httptftp-backdoor/, 2012. (visité le 2015-04-28). (Cité en page 25.)

[88] E. Schmidt. Eric Schmidt Defines Web 3.0. http://readwrite.com/2007/08/07/eric_schmidt_defines_web_30, 2007. (visité le 2015-04-28). (Cité en page 11.)

[89] N. Sidiropoulos and P. Stefopoulos. Smart-TV Hacking. http://delaat.net/rp/2012-2013/p39/report.pdf, January 2013. (Cité en pages 23 et 24.)

[90] SIPSorcery. SIP Password Security - How much is yours worth ? `http://www.sipsorcery.com/mainsite/Help/SIPPasswordSecurity`, 2012. (visité le 2015-04-28). (Cité en page 62.)

[91] SooCurious. HAPIFork : la fourchette intelligente pour apprendre à mieux manger. `http://soocurious.com/fr/hapifork-la-fourchette-intelligente-pour-apprendre-a-mieux-manger/`. (visité le 2015-05-05). (Cité en page 13.)

[92] R. Stallman. The Anonymous WikiLeaks protests are a mass demo against control. `http://www.theguardian.com/commentisfree/2010/dec/17/anonymous-wikileaks-protest-amazon-mastercard`, 2010. (visité le 2015-04-28). (Cité en page 25.)

[93] S. Stamm, Z. Ramzan, and M. Jakobsson. Drive-by pharming. In Sihan Qing, Hideki Imai, and Guilin Wang, editors, *Information and Communications Security*, volume 4861 of *Lecture Notes in Computer Science*, pages 495–506. Springer Berlin Heidelberg, 2007. (Cité en page 25.)

[94] 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. (Cité en page 76.)

[95] A. Stubblefield, J. Ioannidis, and A. D. Rubin. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. In *NDSS*, 2002. (Cité en page 26.)

[96] The Carnegie Mellon University Computer Science Department Coke Machine. The "Only" Coke Machine on the Internet. `https://www.cs.cmu.edu/~coke/history_long.txt`, 1990. (visité le 2015-04-28). (Cité en page 13.)

[97] S. Viehböck. Brute forcing WiFi protected setup. *Wi-Fi Protected Setup*, 2011. (Cité en page 26.)

[98] Vivien. Le retour du combat PPPoA / PPPoE vs IPoA / IPoE. `http://lafibre.info/techno-du-web/pppoa-pppoe-ipoa-ipoe/`, May 11th 2011. (visité le 2015-04-28). (Cité en page 61.)

[99] X. Wang and H. Yu. How to Break MD5 and Other Hash Functions. In *Advances in Cryptology–EUROCRYPT 2005*, pages 19–35, Aarhus, Danmark, May 23rd 2005. (Cité en page 62.)

[100] D. Wing. Network Address Translation : Extending the Internet Address Space. *Internet Computing, IEEE*, 14(4) :66–70, July 2010. (Cité en page 18.)

[101] Xobs and Bunnie. The exploration and exploitation of an sd memory card. In *proc. of 30th Chaos Communication Congress (30C3)*, Hamburg, Allemagne, décembre 2013. (Cité en page 23.)

[102] Hubert Zimmermann. Osi reference model–the iso model of architecture for open systems interconnection. *Communications, IEEE Transactions on*, 28(4) :425–432, 1980. (Cité en page 98.)

Résumé : Aujourd'hui, les équipements intégrant du logiciel et connectés à Internet sont de plus en plus nombreux et variés. Avec l'arrivée de l'"Internet des objets" et la tendance au "tout connecté", de nombreux équipements de notre quotidien bénéficient maintenant d'une connexion à Internet : les Smart-TVs, les lecteurs DVD, les systèmes d'alarmes, les systèmes domotiques, jusqu'aux équipements facilitant l'hospitalisation à domicile de patients par exemple.

Ces évolutions technologiques s'accompagnent malheureusement de problèmes de sécurité. L'utilisation massive du réseau Internet a facilité la propagation de logiciels malveillants, qui peuvent aujourd'hui cibler tout type d'équipement informatique et notamment les équipements connectés. Alors qu'il existe déjà des normes permettant d'évaluer la sécurité d'équipements informatiques industriels, leur application aux équipements grand public est encore limitée. La présence et la criticité des vulnérabilités qui peuvent affecter ces équipements sont encore mal connues car elles n'ont pas fait l'objet d'études approfondies. C'est précisément l'objectif de cette thèse, qui propose une méthode permettant de mener une analyse de vulnérabilités des équipements grand public connectés à Internet. Cette méthode est constituée de deux grandes phases : une phase d'analyse des risques suivie d'une phase d'expérimentations.

L'analyse de sécurité d'un équipement, quelle qu'elle soit, nécessite une bonne connaissance de l'environnement de celui-ci. Afin de guider l'évaluateur dans cette tâche, nous proposons, dans une première phase, de nous fonder sur des méthodes d'analyse des risques existantes. Ces méthodes sont aujourd'hui bien éprouvées et permettent à l'évaluateur d'obtenir une vue globale des risques encourus par l'utilisation de l'équipement étudié. Ensuite, lors de la seconde phase de l'étude, l'évaluateur se concentre sur les risques les plus importants afin de montrer la faisabilité technique des scénarios menant aux risques considérés, à l'aide d'expérimentations. Étant donné le grand nombre et la diversité des connexions présentes sur les équipements connectés, il est important de mettre l'accent sur les scénarios d'attaque qui peuvent s'avérer riches, même si ces scénarios ont pour origine une vulnérabilité locale simple. Pour cette seconde phase, une méthode d'expérimentation est donc proposée pour étudier ces scénarios d'attaque, qui, de plus, ciblent des équipements dont les spécifications ne sont pas forcément disponibles.

Afin d'illustrer la méthode globale, cette thèse se fonde sur deux cas d'étude : les box ADSL et les téléviseurs connectés. Ces études ont été menées sur un panel d'équipements provenant des principaux fournisseurs d'accès à Internet et des principaux fabricants de téléviseurs, ce qui nous a permis de comparer les différents équipements présents sur le marché. Les vulnérabilités mises en évidence concernent en particulier les liens de communication (boucle locale pour les Box ADSL, interface DVB-T pour les Smarts TVs) reliant les équipements à leurs fournisseurs de service (FAI pour les Box ADSL, TV et VoD pour les Smart TVs). Ces liens de communication sont habituellement considérés de confiance et ne sont à notre connaissance pas ou peu étudiés jusqu'à présent. Cette thèse contribue ainsi à l'analyse de

sécurité sur ces liens particuliers des équipements connectés et met en lumière des chemins d'attaque originaux.

Enfin, cette thèse se termine par la présentation des différents mécanismes de protection existants afin d'empêcher l'introduction ou l'exploitation des failles de sécurité identifiées.

Abstract : Today, equipment embedding software and an Internet connection are more and more numerous and various. With the emergence of "the internet of things" and the trend to interconnect everything, many equipment used in our every day life are now connected to the internet: Smart-Tvs, DVD players, alarm and home automation systems, and even health assistance home devices, for example.

Unfortunately, these technological evolutions also introduce new security threats. The massive use of internet facilitates the propagation of malware, capable of targeting any computer device, and more specifically any internet connected device. Although several methods allowing security analysis of industrial systems exist, their application to home devices is still limited. The existence and the criticality of potential vulnerabilities in these devices are not well-known, because they have not been thoroughly studied. This is precisely the objective of this thesis, which presents a method allowing to carry out a vulnerability analysis of internet connected home devices. This method is composed of two main phases: a risk analysis phase followed by an experimental phase.

The security analysis of any type of equipement, requires a good knowledge of its environment. In order to guide the evaluator in this task, we propose, as a first step, to rely on existing risk analysis methods. These methods are now mature, and allow the evaluator to obtain a global view of the risks incurred by the usage of an equipment. Then, during the second step of our method, the evaluator concentrates on the most important risks in order to demonstrate the technical feasibility of the scenarios leading to the considered risks, by carrying out several experiments. Considering the large amount and the diversity of I/Os on connected devices, it is important to focus on specifically rich attack scenarios, possibly depending on a simple local vulnerability. For this second step, an experimental method is proposed in order to study these attack scenarios, which, moreover, target equipement whose specifications are not necessarily available.

In order to illustrate the entire method, this thesis presents two case studies: Integrated Access Devices and Smart-Tvs. These studies are carried out on a panel of devices from major internet service providers and TV manufacturers, allowing us to compare several devices available on the market. The vulnerabilities pointed out, mainly concern the communication means (local loop for the IAD, DVB-T interface for the smart-TVs) connecting these devices to their service providers (ISP for the IAD, TV and VoD for the smart-TVs). These communication links are usually considered safe, and have been, to our knowledge, seldom explored. This thesis thereby contributes to the security analysis of these particular communication means for connected devices and points out some original attack paths.

Finally, this thesis ends by presenting different existing security mechanisms that can be used to avoid exploitation of the identified weaknesses.

Mots clés : Vulnérabilité, UAI, Téléviseur connecté, Analyse de risques, Boucle locale, DVB-T