La sécurité des box ADSL. Analyse de risques et expérimentations

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

La sécurité des box ADSL
Analyse de risques et expérimentations

Yann Bachy [1,2,4], **Vincent Nicomette** [1,2], **Eric Alata** [1,2], **Mohamed Kâaniche** [1,3], **Jean-Christophe Courrège** [4]

1. *CNRS, LAAS, 7 Avenue du colonel Roche, 31400 Toulouse, France*
   prénom.nom@laas.fr
2. *Univ de Toulouse, INSA de Toulouse, LAAS, 31400 Toulouse, France*
   prénom.nom@laas.fr
3. *Univ de Toulouse, LAAS, 31400 Toulouse, France*
   prénom.nom@laas.fr
4. *Thales Communications & Security, 3, avenue de l'Europe, 31400 Toulouse, France*
   prénom.nom@thalesgroup.com

RÉSUMÉ. *La majorité des abonnements à Internet proposés par les fournisseurs français incluent une box permettant à l'utilisateur de bénéficier pleinement de tous les services proposés dans leur offre. L'utilisation de cet équipement réduit considérablement les connaissances techniques nécessaires à l'installation d'Internet au domicile. À notre connaissance, relativement peu d'études ont analysé la sécurité de ces box ADSL. Cet article présente 1) une analyse des risques de ce type d'équipement, conduite à l'aide de la méthode EBIOS et 2) des expérimentations visant à mettre en œuvre un scénario d'attaque correspondant à un des risques identifiés lors de la phase d'analyse. La première partie de cet article décrit l'analyse de risques, et identifie un scénario d'attaque qui nous mène à étudier la boucle locale. La deuxième partie de l'article met en œuvre cette attaque, en proposant une plateforme permettant d'intercepter et d'analyser tous les protocoles réseaux mis en œuvre lors du démarrage d'une box ADSL. Cette plateforme a mis en évidence un problème de sécurité potentiel pour deux box parmi celles étudiées. Nous présentons ensuite une expérimentation illustrant une exploitation concrète des faiblesses identifiées.*

ABSTRACT. *Many French Internet providers include an ADSL box in their offers allowing the customer to easily take advantage of all the services included in the offer. This equipment drastically reduces the technical skills required to install the Internet connection at home. But, to our knowledge, very few studies propose to evaluate the security of these ADSL boxes. This is the purpose of this paper. This paper presents 1) a risk analysis of such equipment, following the EBIOS methodology, and 2) experiments aiming to illustrate the existence of an attack*

Ingénierie des systèmes d'information – n° 6/2014, 63-88

scenario corresponding to one of the risks identified during the analysis. The first part of this paper describes the risk analysis, which allowed us to identify a risk leading us to study the local loop. The second part introduces a novel method allowing us to sniff and analyze all the network protocols used during the boot-up sequence of ADSL boxes. This study allowed us to identify a potential security problem for two of the boxes we have analyzed. Finally we present a platform illustrating possible exploitations of these weaknesses.

MOTS-CLÉS : *box, ADSL, DSLAM.*

KEYWORDS: *box, ADSL, DSLAM.*

DOI:10.3166/ISI.19.6.63-88

1. Introduction

L'Internet grand public date du début des années 1990. En seulement quelques années, il est devenu bien plus qu'un simple outil de travail à domicile. Ce réseau est devenu une nouvelle source de loisirs et de communication au quotidien. En parallèle, Internet est devenu de plus en plus accessible, tant d'un point de vue technique qu'économique. De plus, depuis les années 2000, la vision que l'on avait usuellement du réseau Internet s'est considérablement modifiée. On parle maintenant d'« Internet des objets », d'objets communicants, de systèmes cyber-physiques. De plus en plus d'équipements de toute sorte, connectés au réseau Internet, envahissent notre quotidien professionnel mais aussi notre domicile. Les téléphones bien sûr, mais aussi les systèmes d'alarmes, les caméras de surveillance, les systèmes domotiques, les lecteurs DVD, les téléviseurs, même certains réfrigérateurs possèdent aujourd'hui une connexion au réseau Internet.

Malheureusement, le développement rapide de ces objets connectés n'a pas été accompagné d'une étude rigoureuse et systématique de leur sécurité. Il est donc fort probable que ces derniers contiennent un certain nombre de vulnérabilités. Des récentes découvertes de vulnérabilités sur ce genre d'équipements, telles que le *botnet* identifié il y a quelques mois, qui contenait des routeurs grand public, des centres multimédias, Smart-TV et réfrigérateurs (Proofpoint, 2014), en sont la preuve.

Il est donc très difficile aujourd'hui de pouvoir utiliser ces différents équipements connectés en ayant une bonne connaissance des risques que l'on prend en les intégrant à une infrastructure existante, à la fois dans le monde professionnel, mais aussi dans le monde privé. Pourtant, différentes méthodes d'analyse de risques existent et pourraient être systématiquement utilisées pour évaluer la sécurité de ces différents équipements.

Dans le cadre de cette étude, nous avons choisi d'étudier l'équipement connecté qui est aujourd'hui central dans chaque domicile : la box ADSL (*Asymmetric Digital Subscriber Line*). Cet objet est en général le point d'entrée de la connexion à Internet du domicile ou des petites entreprises (ne possédant pas de liaison dédiée). Sa sécurité est donc primordiale.

Les box ADSL sont aujourd'hui très répandues, et de plus en plus simples à installer et à configurer. Nul besoin aujourd'hui de connaissances techniques avancées pour installer une connexion Internet à son domicile : tous les opérateurs fournissent des guides d'installation ainsi qu'une aide téléphonique, facilitant grandement l'installation de la connexion Internet. Afin d'attirer de nouveaux clients, les opérateurs ont inclus de nouveaux services tels que la téléphonie et la télévision en s'inspirant des offres « *triple play* » introduites aux États-Unis à la fin des années 1990. Tous ces services se trouvent désormais inclus dans les dernières générations de box ADSL, qui sont par conséquent de plus en plus complexes. Le développement de ces box est propre à chaque opérateur. Cependant, on peut globalement la définir ainsi : une box regroupe l'ensemble des dispositifs nécessaires à l'utilisation des différents services proposés par son fournisseur d'accès. Ces box permettent donc d'accéder à Internet, mais contiennent bien d'autres services tels que la TV ou un point d'accès wifi. L'installation du réseau informatique à la maison s'en trouve grandement facilitée, grâce également à la fonctionnalité de traduction d'adresse réseau (NAT [1]) qui est incluse dans ces box. De ce fait, tous les ordinateurs peuvent accéder à Internet simultanément. Tout ceci conduit à l'émergence de protocoles réseaux grand public tels que DLNA [2], conduisant à un haut niveau de partage des données et une augmentation de communications numériques entre les équipements que les utilisateurs peuvent connecter à l'Internet.

Tout comme pour d'autres équipements informatiques embarqués (Cui *et al.*, 2008), il est donc important de s'interroger sur la sécurité de ces box ADSL. L'ANSSI [3] s'inquiète ("Défense et sécurité nationale", 2013) de la possibilité de détourner ces équipements pour constituer un gigantesque *botnet* [4]. Plusieurs vulnérabilités ont déjà été identifiées (Ruff, 2006 ; Raynal, Campana, 2012 ; Geissler, Ketelaar, 2013). Cependant, toutes ces études ne prennent en compte que deux cas de figure : 1) l'attaquant est l'utilisateur lui-même, il possède un accès physique à l'équipement, et il peut faire ce qu'il veut ; 2) l'attaquant est sur un site distant et tente d'accéder à la box à travers Internet. Nous allons montrer dans notre étude que d'autres stratégies d'attaques peuvent être utilisées.

A notre connaissance il n'existe, à ce jour, pas d'étude globale des problèmes de sécurité d'une box. Afin de pallier à ce manque, nous avons décidé d'établir cette analyse, ce qui constitue la première partie de cet article. Nous avons pour cela utilisé une méthodologie issue du monde industriel : l'analyse de risques. Elle permet, d'une manière rigoureuse, de traiter chaque composante du système. Il existe plusieurs méthodologies d'analyse de risques (MEHARI (CLUSIF, 1997), OCTAVE (CERT, 1999), EBIOS (ANSSI, 1995)). Nous avons décidé d'utiliser EBIOS car elle a été développée par l'ANSSI, entité étatique française et constitue une référence sur le territoire

1. *Network address translation.*
2. *Digital Living Network Alliance.*
3. Agence nationale de la sécurité des systèmes d'information.
4. Réseau de robots informatiques.

français. Le déroulement de la méthodologie EBIOS sur notre cas d'étude, nous a permis de définir les différents risques liés à l'utilisation des box. Les résultats nous ont notamment permis de révéler l'importance de la sécurité de l'infrastructure reliant l'abonné à l'opérateur. Ceci nous a conduit à envisager une attaque, dans laquelle l'attaquant opère directement sur la ligne téléphonique reliant l'abonné à l'opérateur.

La deuxième partie de cet article propose une expérimentation mettant en oeuvre cette attaque et décrit deux plateformes que nous avons conçues et implémentées à cette fin. La première plateforme permet d'écouter passivement toute communication entre une box ADSL et Internet. À l'aide de cette plateforme, nous nous sommes interessés aux protocoles mis en œuvre entre la box et les serveurs de l'opérateur, lors du démarrage de la box, et ce pour la plupart des box actuellement en service. Ces communications se révèlent très importantes car elles caractérisent la procédure de configuration d'une box. L'analyse de ces communications nous a permis d'identifier et de comparer avec précision les protocoles utilisés par les box françaises lors de la phase de configuration et, en particulier, d'identifier des faiblesses dans deux box. La seconde plateforme permet d'émuler le réseau d'un opérateur et ainsi de d'illustrer des attaques possibles permettant de tirer profit des faiblesses précédemment identifiées.

Cet article est organisé comme suit. La section 2 présente l'analyse de risques que nous avons conduite. Ces travaux, nous ont permis de mettre en évidence, la faiblesse de l'utilisation de la boucle locale pour la sécurité des box. La section 3 décrit, d'une part, une plateforme permettant d'écouter le trafic entre une box et le fournisseur d'accès à Internet, et d'autre part, les résultats de la campagne d'écoute que nous avons menée à l'aide de cette plateforme. Cette experimentation a mis en évidence quelques faiblesses susceptibles d'être exploitées dans les protocoles mis en œuvre lors de la phase de démarrage de certaines box. La section 4 présente une seconde plateforme conçue pour exploiter ces vulnérabilités. Enfin, la section 5 propose quelques perspectives à nos travaux.

2. Analyse de risques

Pour mener à bien cette analyse de risques, nous suivons la méthodologie EBIOS 2010 [5]. Nous traitons uniquement les quatre premières étapes prévues dans cette méthodologie, ce qui nous permet d'identifier les principaux risques du contexte étudié. Nous abordons la cinquième étape lors de la conclusion de cet article, en proposant plusieurs contre-mesures.

Dans cette partie nous présentons la méthodologie EBIOS, puis nous établissons le contexte de l'étude, pour ensuite traiter les événements redoutés et les scénarios de menaces. Finalement, dans une dernière partie, nous présentons les différents risques associés à l'utilisation d'une box.

5. Expression des Besoins et Identification des Objectifs de Sécurité, méthodologie proposée par l'ANSSI en 1995 et revue en 2010 en collaboration avec le « club EBIOS ».

2.1. Présentation générale d'EBIOS

La figure 1 présente la démarche décrite dans la méthodologie EBIOS. La démarche EBIOS se veut itérative, permettant de faire plusieurs fois appel à chaque module afin d'améliorer progressivement les résultats de l'étude. Nous présentons ici les 5 modules qui guident notre analyse de risques.

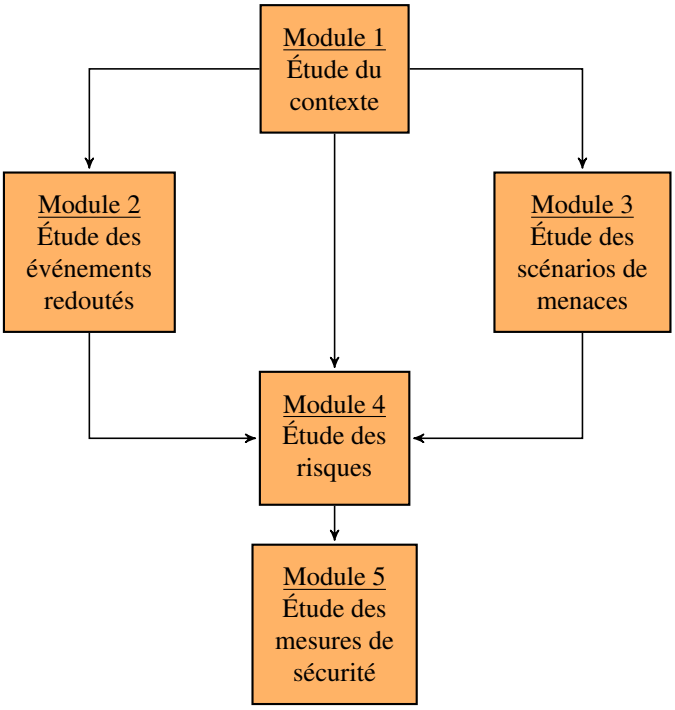

Figure 1. La démarche itérative d'EBIOS

Le module 1 consiste à définir le contexte de l'étude. Cette définition 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 (termes définis dans EBIOS sur lesquels nous reviendrons par la suite) ainsi que les mesures de sécurité existantes à prendre en compte dans le traitement des risques. Les modules 2 et 3 contribuent chacun à l'appréciation des risques. Le module 2 formule les événements redoutés en identifiant les besoins de sécurité des 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. Le module 3 identifie les scénarios pouvant engendrer les événements redoutés. Pour cela, ce module étudie les menaces que peuvent générer les sources de menaces et les vulnérabilités exploitables. Le quatrième module confronte les événements redoutés aux scénarios de menaces permettant ainsi

d'obtenir les différents risques du système. Le module 5 permet finalement de traiter les risques en proposant des mesures de sécurité à mettre en œuvre.

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

2.2. Contexte de l'étude

2.2.1. Objectifs et cadre de l'étude

Le but de cette analyse est de définir les risques associés à l'utilisation des box incluses dans les offres « triple play ». Pour cette étude, nous considérons une utilisation privée de la box, et nous réalisons cette étude du point de vue de l'utilisateur.

Nous nous intéressons uniquement à l'IAD [6], « boîtier modem ». La STB [7], « 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 accès au réseau téléphonique en dehors de ce périmètre.

Dans le contexte des box nous avons identifié les 7 `sources de menaces` présentées dans le tableau 1. Nous avons décidé de ne pas différencier ces sources de menaces selon leur `capacité`, pour simplifier l'étude dans un premier temps [8]. 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.

2.2.2. Définition des métriques

Tout au long de l'étude, nous utilisons différentes échelles, qu'il faut donc définir au préalable. 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 box, nous avons jugé pertinent d'inclure également la propriété d'*authenticité*. Pour chaque critère de sécurité, il est ensuite nécessaire de définir une échelle des `besoins`. Les 4 critères avec leur échelle de besoins respective sont présentés dans le tableau 2. Il est à noter que ces échelles doivent représenter le besoin et la tolérance de l'utilisateur.

---

6. *Integrated Access Device.*

7. Set-Top Box.

8. Classiquement, la méthodologie EBIOS prévoit 3 niveaux de capacités : Faibles, Importantes et Illimitées.

Tableau 1. Sources de menaces

Source 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 physiques	✓	Ext	✓
Abonné	✓	Int	
Opérateur	✓	Ext	
Virus[a]		Ext	✓
Problèmes météorologiques		Ext	

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

Des échelles standard sont proposées dans le référentiel EBIOS, nous nous sommes inspirés de ces échelles pour construire les nôtres.

Tableau 2. Critères de sécurité

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		**Déscription**
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

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 et 4.

Tableau 3. Échelle de gravité

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

Tableau 4. Échelle de vraisemblance

	Niveau	**Déscription**
1	Minime	Une fois tous les 5 ans
2	Significative	Une fois par an
3	Maximale	Journalier

2.2.3. Identification des biens

Une analyse de risques, suivant la méthodologie 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, supports aux biens essentiels précédemment identifiés. Un système peut également déjà avoir intégré des mesures de sécurité. La méthode EBIOS préconise de les identifier, dans le contexte de l'étude. Dans notre cas, les biens essentiels sont les fonctionnalités primaires de la box :

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 des différents biens supports. Ces biens supports sont regroupés en différentes catégories dans EBIOS [9]. Dans cette étude nous avons identifié des biens supports de 5 types :

1) **Matériels** : alimentation électrique, disque dur.
2) **Organisations** : FAI [10].
3) **Réseaux** : boucle locale, Femto [11], liaison IAD/STB, réseau local, WiFi.

9. Locaux, systèmes, matériels, logiciels, réseaux, organisations, personnes, papiers, canaux interpersonnels.

10. Fournisseur d'accès à internet.

11. Mini antenne-relais GSM permettant d'améliorer le signal GSM à domicile.

4) **Personnels** : abonné.

5) **Logiciels** : services réseaux WAN [12] [13], services réseaux LAN [14] [15], contrôle parental.

Plusieurs biens supports pouvant servir à différents biens essentiels, le tableau 5 présente la correspondance entre ces différents biens.

Tableau 5. Relations entre biens essentiels et biens supports

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

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 méthodologie EBIOS et vont permettre de réduire ou d'annuler les risques concernés par ces mesures de sécurité. Pour les box, nous avons identifié 5 mesures de sécurité existantes :

1) **Identification** de la box. Cette identification varie en fonction des opérateurs, elle peut être faite soit par une combinaison de identifiant/mot de passe, soit par vérification de l'adresse MAC [16] 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 la box. Cette mesure permet de protéger la box contre la météo (hors phénomènes électromagnétiques) mais aussi contre un accès physique sans autorisation. Ceci permet de réduire le risque d'attaques matérielles directement sur la box.

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.

12. *Wide Area Network*.
13. On regroupe ici tous les logiciels côté WAN : filtrage / firewall, NAT et l'administration de ces services.
14. *Local Area Network*
15. On regroupe ici tous les logiciels côté LAN : DHCP, DNS et l'administration de ces services.
16. *Media access control* : adresse physique.

4) **Cloisonnement WiFi invité**. De nombreuses box 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 box est équipée d'un filtre de paquets (pare-feu) empêchant un accès depuis un réseau extérieur à la box.

2.3. 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. Le besoin de sécurité correspond au niveau attendu de sécurité (ces besoins ont été définis dans le tableau 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.

en cas de 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.

Plutôt que de lister ici ces 4 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 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 ici donc de fournir le point de vue d'un utilisateur de la box. La variété de profils d'utilisateurs d'une box nous a contraint a définir un profil pour notre étude. Le profil type que nous décidons d'adopter est celui d'un père de famille n'ayant pas d'attrait particulier pour l'informatique. Dans ce cas précis nous considérons par exemple 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).

Tableau 6. Gravité de l'impact en cas de manquement au besoin de sécurité

	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

Les deux exemples que nous retenons sont :

WEB - Confidentialité

– Besoin de sécurité : 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 [17] : opérateur, personne extérieure malveillante réalisant des attaques réseaux, personne extérieure malveillante réalisant des attaques physiques, 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

– Besoin de sécurité : 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 physiques, 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).

2.4. Étude des scénarios de menaces

L'étude des scénarios de menaces consiste à déterminer la vraisemblance de toutes

17. 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 est aujourd'hui systématiquement actif.

les menaces associées à chaque critère de sécurité d'un bien essentiel. Il existe, dans le référentiel EBIOS, des types de menaces associés à chaque classe de biens supports. Certaines classes, 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 et 3) le niveau de vraisemblance de mise à exécution de la menace.

Pour cela, au lieu de donner la liste de ces 3 éléments pour chaque bien support et chaque critère de sécurité, nous préférons détailler trois exemples également présentés dans le tableau 7, qui indique le niveau de vraisemblance de mise à exécution de la menace pour chaque bien support et chaque critère de sécurité [18].

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.

Les trois exemples retenus sont les suivants :

Boucle locale - Confidentialité

– Sources de menaces : personne extérieure malveillante réalisant des attaques physiques.

– Menaces : divulgation du contenu.

– Vraisemblance : minime.

FAI - Authenticité

– Sources de menaces : personne extérieure malveillante réalisant des attaques physiques, personne extérieure malveillante réalisant des attaques réseaux.

– Menaces : usurpation d'identité.

– Vraisemblance : significative.

18. Le contenu de ce tableau résulte notamment de l'expertise du personnel expert du CESTI Thales ayant participé à cette étude.

Services réseaux WAN - Disponibilité

– Sources de menaces : personne extérieure malveillante réalisant des attaques physiques, personne extérieure malveillante réalisant des attaques réseaux, utilisateur interne malveillant, abonné, virus.

– Menaces : logiciel indisponible, logiciel supprimé.

– Vraisemblance : significative.

Tableau 7. Niveau de vraisemblance de mise à exécution des menaces

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 IAD / 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	-	-

2.5. Étude des risques

La dernière étape de notre analyse de risques consiste à établir 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 les 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 84 risques. Pour les obtenir, il suffit de considérer les trois tableaux 5, 6 et 7. Prenons l'exemple dans le tableau 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 5), et de compter ceux pour lesquels des menaces identifiées relatives à l'indisponibilité sont présentes dans le tableau 7

(quelle que soit leur vraisemblance). Il y en a 9. En utilisant la même méthode pour toutes les cases du tableau 6, on obtient ainsi au total 84 risques. Cette méthode est à privilégier lorsqu'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 trois tableaux 5, 6 et 7. Prenons le même exemple, correspondant à l'intersection du bien essentiel web et du critère *disponibilité* dans le tableau 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 7 correspondant aux biens support du web (qui sont au nombre de 10, comme indiqué dans le tableau 5). Parmi les 9 scénarios de menaces correspondants, 5 ont une vraisemblance *Minime* et 4 ont une vraisemblance *Significative* [19]. 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 *Important*, 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 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.

Tableau 8. Analyse des risques

	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	
Important	TEL non confidentiel	TEL non intègre WEB non disponible	WEB non authentique
Critique		TEL non disponible NAS non intègre WEB non confidentiel	

Le tableau 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 la gravité est *Critique* et la vraisemblance *Significative* ou

19. 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.

Maximale, ainsi que les risques dont la vraisemblance est *Maximale* et la gravité *Important* ou *Critique*. 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 4 risques, on constate 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 investiguer 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 dans le contexte de box ADSL nous a été utile dans la mesure où elle nous a permis d'envisager un scénario d'attaque original et différent des travaux existants (Ruff, 2006 ; Raynal, Campana, 2012 ; Geissler, Ketelaar, 2013). Ces trois travaux présentent essentiellement des méthodes permettant de compromettre une box. Les sources de menaces mises en jeu dans ces travaux sont l'*utilisateur interne malveillant*, la *personne extérieure malveillante réalisant des attaques sans accès physique* et les *virus*. Les scénarios de menaces envisagés concernent l'*intégrité* des *services réseaux WAN*, l'*intégrité* des *services réseaux LAN*, la *confidentialité* du *réseau local* et l'*intégrité* du *FAI*. Dans le premier article (Ruff, 2006), l'auteur s'intéresse également aux risques associés à une compromission. L'auteur suggère dans un premier temps la possibilité que la box puisse servir dans un botnet ou de relais de spam, qui relèvent du risque *WEB non intègre* du point de vue de l'opérateur. Dans un second temps, il suggère que la compromission d'une box permet à l'attaquant d'écouter tout le trafic correspondant à un utilisateur, ce qui relève du risque *WEB non confidentiel*. Si toutefois des inquiétudes concernant la confidentialité sont évoquées, il n'est jamais fait mention d'attaques physiques portant directement sur la boucle locale.

Dans la suite de cet article nous nous intéressons donc à cette boucle locale et à la place qu'elle occupe dans la sécurité des réseaux domestiques. Afin de tester les éventuelles faiblesses des box ADSL vis-a-vis de cette boucle locale, nous avons conçu et implémenté une plateforme permettant d'observer les échanges réalisés sur ce tronçon du réseau. La section suivante présente cette plateforme. Grâce à cette plateforme nous avons pu identifier une vulnérabilité intéressante que nous avons pu exploiter avec succès. Cette exploitation fait l'objet de la section 4.

3. Plateforme d'observation de communications ADSL

Notre premier objectif a été de proposer une plateforme capable d'écouter toutes les communications sur la boucle locale, en particulier celles qui concernent la phase de démarrage d'une box. Cette plateforme est composée d'un DSLAM [20] et d'un MoDem ADSL [21]. Dans cette section nous rappelons dans un premier temps le fonctionnement de la boucle locale. Puis nous décrivons notre plateforme. Enfin, une dernière partie est dédiée à la présentation de l'étude comparative que nous avons menée sur la séquence de démarrage des différentes box.

3.1. La boucle locale

Tous les opérateurs français présentent globalement la même architecture d'accès réseau. Ils possèdent chacun leur propre cœur de réseau. Afin de relier l'abonné à ce réseau, la majorité utilisent des réseaux existants tels que le réseau téléphonique historique, aussi appelé boucle locale. Cette méthode a pour avantage d'atteindre facilement la majorité des foyers français sans devoir déployer un réseau supplémentaire jusqu'à l'abonné. Il existe principalement 4 types de supports physiques utilisés pour la boucle locale : la paire de cuivre, les fibres optiques, le câble coaxial et les ondes radio [22]. Dans la suite de cet article nous nous intéressons uniquement à la paire de cuivre, installée par l'opérateur historique, qui reste aujourd'hui le support le plus utilisé en France [23]. En effet, au troisième trimestre 2013, l'ARCEP [24](“Observatoire trimestriel des marchés de détail des communications électroniques (services fixes haut et très haut débit) en France - 3e trimestre 2013”, 2013) stipule que 91% des connexions, à l'Internet haut et très haut débit, se font en utilisant la paire de cuivre (technologies xDSL).

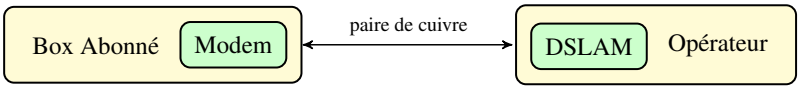

Figure 2. La boucle locale

La paire de cuivre est reliée côté abonné à un MoDem et à un DSLAM côté opérateur (cf. figure 2). Ces deux équipements modulent et démodulent un signal analogique, transmis sur la paire de cuivre à haute fréquence, en signaux numériques (et inversement).

---

20. *Digital Subscriber Line Access Multiplexer.*
21. Modulateur et Demodulateur ADSL.
22. On regroupe ici le WiMax, WiFi et les connexions satellites.
23. Cette méthode peut également s'appliquer aux autres supports, en particulier sur une boucle radio, moyennant les équipements adéquats.
24. Autorité de régulation des communications électroniques et des postes.

Par la suite, nous décrivons une plateforme destinée à analyser la sécurité des communications entre le fournisseur d'accès à Internet et la box sur la boucle locale. Cette plateforme a été conçue et implémentée de manière à permettre l'observation du trafic envoyé et reçu par la box sur la boucle locale.

3.2. Description de la plateforme

Afin de capturer toutes les données 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 ("Man in the Middle")* : 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 de nos travaux. 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.

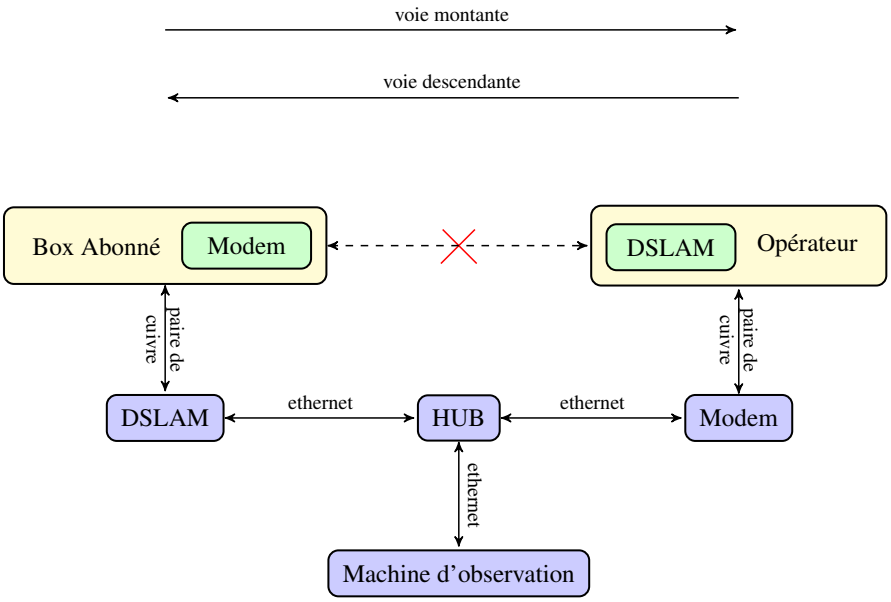

Figure 3. Écoute sur la boucle locale

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 (voir figure 3). 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 la box ADSL 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 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 (voir figure 3). Comme l'écoute sur un réseau Ethernet est très facile, les communications envoyées et reçues par la box peuvent être étudiées.

Cette configuration nous a permis de procéder à une étude comparative sur les différents protocoles mis en œuvre lors de la phase de démarrage des différentes box déployées en France.

3.3. Résultats

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 [25].

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 la box étudiée, et se compose de quatre étapes (détaillées par la suite) : 1) ATM [26], 2) PPP, 3) Configuration et 4) SIP.

Tous les résultats de cette étude sont rassemblés dans le tableau 9. La première colonne contient l'identifiant de la box (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'authen-

25. 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.

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

tification est utilisé. La quatrième colonne indique si l'opérateur utilise le protocole DHCP afin d'attribuer une adresse IP à la box. 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.

Tableau 9. Caractéristiques des différentes box ADSL déployées en France

Box	ATM	PPP	DHCP	SIP	Configuration	Mise à jour
A	8/35/LLC	chap	no	MD5	HTTP, FTP, SSL	-
B	8/35/LLC	chap	yes	MD5	HTTP, SSL	SSL
C	8/36/VC	no	yes	MD5	SSL	-
D	8/35/LLC	chap	yes	MD5	HTTP	HTTP
E	8/35/LLC	chap	yes	MD5	HTTP	HTTP
F	8/35/LLC	chap	no	MD5	SSL	-

3.3.1. 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 la box fournie par l'opérateur. À l'issue de nos observations, seules 4 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-conception.

3.3.2. PPP

Ce protocole est fréquemment utilisé lorsque les opérateurs doivent partager la boucle locale (Vivien, 2011) 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.

3.3.3. SIP

Le protocole le plus fréquemment utilisé pour la téléphonie sur IP, et donc sur Internet, est SIP. Un client SIP, qui dans notre cas est inclus dans la box, 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 4 :

– 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 *empreinte* MD5 [27] calculée principalement à partir du *nonce* et du mot de passe SIP (que le client SIP connaît ou est capable de calculer).

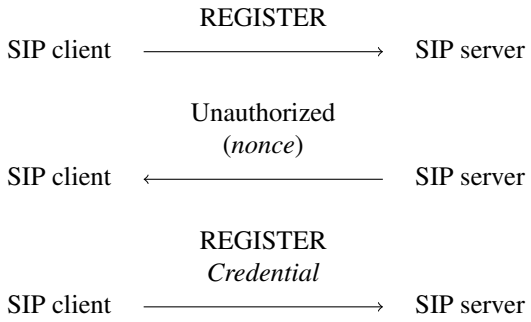

Figure 4. Enregistrement SIP - HTTP Digest

Bien que l'utilisation de l'algorithme de hachage MD5 soit déconseillée depuis plusieurs années déjà, à cause de certaines vulnérabilités prouvées (Wang, Yu, 2005), toutes les box utilisent MD5 pour générer l'*empreinte* de leurs réponses.

Cependant, en considérant que 1) le *nonce* varie régulièrement (SIPSorcery, 2012), 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.

3.3.4. Configuration

Les box 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.

La configuration d'une box 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 la box 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. De plus, la requête DNS révèle d'importantes informations concernant l'échange. Par exemple,

27. *Message Digest 5*.

si le nom de domaine du serveur contacté contient le terme TR69 [28] ou un équivalent, il est raisonnable de supposer que ces échanges concernent la phase de configuration.

Les protocoles utilisés, afin de transmettre la configuration, sont présentés dans l'avant-dernière colonne du tableau 9. Nous constatons que les différents opérateurs n'utilisent pas tous les mêmes protocoles pour envoyer à la box sa configuration. La plupart des fournisseurs utilisent le protocole sécurisé HTTPS [29]. Pour les box 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 recommendations émises par l'ANSSI (Levillain, 2012). Cependant, lorsque nous nous intéressons aux boxs D et E, nous pouvons voir que seul le protocole non sécurisé HTTP est utilisé. Cette faille de sécurité nous permet, pour ces deux box, d'extraire la configuration lors de leur démarrage. Il est à noter que cette faille est exploitable car les données échangées ne sont pas signées. L'utilisation d'une signature nous permettrait uniquement de lire l'échange, et non de le modifier.

3.3.5. Mise à jour

Plusieurs box 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 box vérifient la présence d'un nouveau firmware automatiquement lors du démarrage de la box. 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 box D et E n'est pas sûre. Comme lors de la phase de configuration, nous sommes capables d'extraire et/ou de modifier le *firmware* lors de cette procédure.

3.3.6. Observations

Pour résumer ces expérimentations, globalement, les principales box françaises fonctionnent de la même manière. Cependant, certaines box diffèrent significativement des autres sur un point : la protection des phases de configuration et de mise à jour. Dans la suite de cet article nous nous intéressons aux conséquences des faiblesses présentes dans les protocoles mis en œuvre entre l'opérateur et la box. Nous nous appuyons sur les résultats obtenus et nous définissons une méthode itérative afin d'explorer les conséquences de ces faiblesses.

---

28. TR69 ou CWMP : *CPE WAN Management Protocol*.
29. *Secure HTTP*

4. Plateforme d'imitation d'un fournisseur d'accès à Internet

Afin d'analyser plus en détail les protocoles mis en œuvre entre l'opérateur et la box, nous avons simulé le comportement du fournisseur d'accès à Internet. En effet, 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 réseau de l'opérateur (voir figure 5). Nous avons installé et configuré les différents éléments au fur et à mesure, en suivant une méthode iterative. Dans la suite nous présentons notre méthode itérative accompagnée de quelques exemples, puis nous donnons les résultats que nous avons obtenus en appliquant cette méthode à l'analyse de sécurité de la phase de mise à jour.

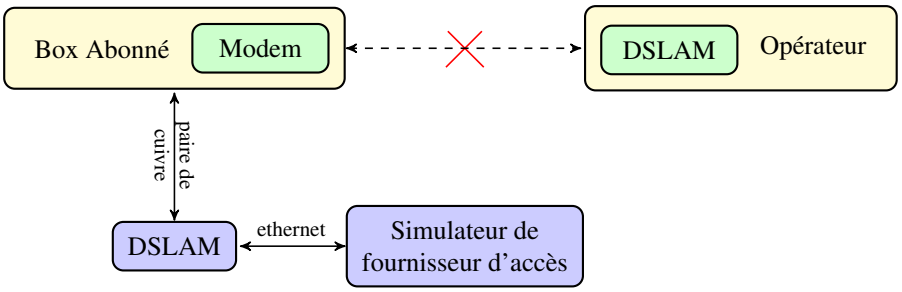

Figure 5. Simulation d'un fournisseur d'accès à Internet

4.1. Méthode itérative

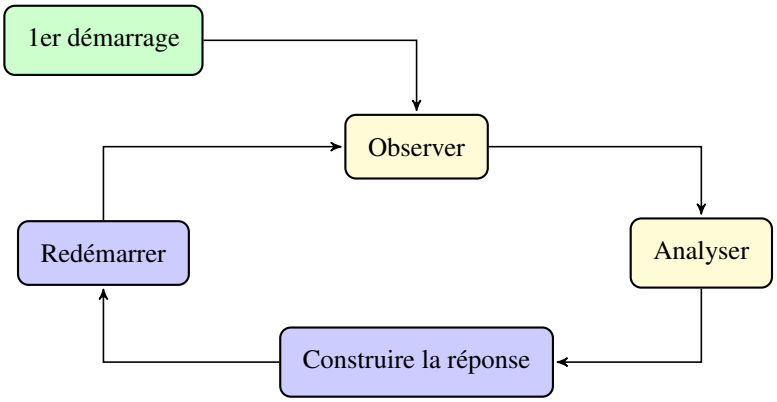

Figure 6. Méthode itérative

Notre méthode d'analyse est une approche de type boîte grise. En effet, nous n'avons aucune connaissance particulière sur le fonctionnement interne du système que nous avons étudié. Toutefois, les résultats de notre première étude (cf. section 3.3) nous ont donné de précieuses informations facilitant cette seconde étude. Notre méthode se déroule en quatre étapes répétées de manière cyclique (voir figure 6).

– **Observer** : après le démarrage de la box, nous observons les requêtes émises par celle-ci sur le lien réseau la reliant à l'opérateur ;

– **Analyser** : nous analysons les requêtes qui semblent empêcher la box de poursuivre son démarrage. Souvent ces requêtes sont émises à intervalle régulier en attendant une réponse ;

– **Construire la réponse** : nous installons et configurons les logiciels nécessaires permettant de répondre à la dernière requête reçue ;

– **Redémarrer** : nous redémarrons la box de façon à procéder à une nouvelle séquence de démarrage.

Ces quatre étapes sont exécutées itérativement jusqu'au démarrage complet de la box.

4.2. Services mis en œuvre

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

– **PPP** : au démarrage, pour les opérateurs utilisant PPP, les box cherchent d'abord à s'authentifier auprès de l'opérateur selon le protocole PPP.

– **DNS** : des équipements embarqués, tels que les box, 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 la box d'initier ses requêtes.

4.3. Résultats

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, de ce fait la box refuse systématiquement de communiquer avec notre plateforme. Ce problème ne se pose pas avec le protocole non sécurisé HTTP. En nous inspirant des informations obtenues lors de notre première étude, nous sommes parvenus à créer notre propre mise à jour et à l'installer au sein de la box. 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 la box.

Ces trois modifications permettent de contrôler entièrement la box 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 surtaxés seront facturés. Il est important de noter que les conditions d'attaque permettant d'aboutir à ces résultats sont relativement difficiles à obtenir, ce qui rend l'attaque peu probable. Il y a bien évidemment un aspect financier qui entre en jeu, mais l'attaquant a également besoin de pouvoir identifier chaque paire de cuivre traversant une gaine. Si ces attaques restent relativement simples à mettre en œuvre, les conditions nécessaires les rendent assez peu probables, même si leurs effets peuvent être critiques, comme nous le montrons dans cet article. Les résultats obtenus par le biais de ces expériences confirment donc bien les conclusions de l'analyse EBIOS réalisée dans la section 2.

5. Conclusion

Des entités étatiques telles que l'ANSSI sont préoccupées par la sécurité des différentes box, et la possibilité pour un attaquant de créer et déployer depuis l'Internet, par exemple, un immense botnet utilisant toutes les box déployées en France. À cette date et à notre connaissance, très peu d'études scientifiques se sont intéressées à la sécurité de ces box, alors qu'une grande partie de la sécurité des réseaux domestiques français repose sur ces box. Dans cet article, nous avons mené une analyse de risques sur les box de manière générale, en suivant la méthodologie EBIOS. Cette méthodologie a pour avantage d'être exhaustive et reconnue par les industriels. Nous avons identifié 15 risques à l'issue de cette analyse, que nous avons classés en quatre niveaux. Le niveau le plus élevé contient 4 risques qui nous ont orientés vers une étude de la boucle locale. Nous avons proposé deux méthodes innovantes permettant d'analyser la sécurité de la boucle locale dans le cadre des équipements d'accès à Internet de nouvelle génération. Ces deux méthodes ainsi que les premiers résultats nous conduisent à apporter deux contributions :

– Une première plateforme permettant d'observer toutes les communications entre toute box et les serveurs de l'opérateur, en particulier lors des phases de configuration et de mise à jour. Ces observations nous ont permis de comparer les protocoles mis en œuvre lors de ces deux phases et surtout d'identifier des faiblesses sur deux box.

– Une deuxième plateforme permettant d'approfondir l'analyse de sécurité et d'exploiter les faiblesses identifiées.

La dernière étape de l'analyse EBIOS concerne l'`Etude des mesures de sécurité`. Dans cette partie il est question de traiter les risques. Il est possible de proposer certaines mesures de sécurité ou bien d'accepter les risques. Dans le cadre de cette étude nous préconisons plusieurs mesures de sécurité permettant de limiter les risques identifiés.

La première mesure de sécurité proposée concerne l'utilisation de protocoles sécurisés comme HTTPS. Dans cette étude nous avons pu voir que la majorité des opé-

rateurs a déjà opté pour le protocole sécurisé HTTPS. Lorsque ce protocole est correctement implémenté, les attaques présentées dans cet article deviennent beaucoup plus complexes, voire impossibles.

La seconde mesure de sécurité exploite les propriétés physiques d'une infrastructure comme Internet. En effet, à l'aide de l'atténuation du signal, une box est capable de calculer la distance qui la sépare de son DSLAM. Cette valeur devrait drastiquement varier lorsqu'une plateforme telle que la nôtre est insérée sur la boucle locale. Cette mesure permettrait de détecter de manière générale toute interruption d'une ligne et ainsi éviter les tentatives d'écoute. Il est certain que cette mesure ne permet pas d'empêcher chaque tentative d'attaque. Il suffirait pour l'attaquant d'amplifier le signal afin d'influencer ce calcul. Néanmoins, le coût d'intégration de cette contre-mesure nous semble négligeable, et permet d'augmenter significativement l'effort à fournir par l'attaquant.

La troisième et dernière mesure de sécurité proposée concerne plus directement les firmware. Ces derniers sont directement fournis par les opérateurs et transmis par la boucle locale. Il est essentiel de pouvoir s'assurer que ces firmwares n'ont pas été altérés lors de leur transmission. Pour cela il est essentiel d'utiliser des méthodes de signature du firmware.

Suite à ces travaux, nous menons actuellement des analyses similaires sur d'autres équipements grand public connectés à Internet, tels que les téléviseurs et lecteurs Blu-Ray connectés.

Remerciements

Nous tenons à rendre hommage à Yves Deswarte, Directeur de Recherche au sein de l'équipe Tolérance aux fautes et sûreté de fonctionnement au LAAS-CNRS, décédé en 2014, pour sa participation et ses contributions aux travaux effectués sur ce thème.

Bibliographie

ANSSI. (1995). Ebios. http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html.

CERT. (1999). Octave. http://www.cert.org/octave/.

CLUSIF. (1997). Mehari. http://www.clusif.asso.fr/fr/production/mehari/.

Cui A., Costello M., Stolfo S. J. (2008, April 23rd). When firmware modifications attack: A case study of embedded exploitation. In *proc. of network and distributed system security symposium (ndss).* San Diego, USA.

Défense et sécurité nationale. (2013). In, p. 44–45. Paris, France http://www.elysee.fr/assets/pdf/Livre-Blanc.pdf, Direction de l'information légale et administrive.

Geissler P., Ketelaar S. (2013, April 11th). How i met your modem: Advanced exploitation & trojan development for consumer dsl devices. In *proc. of hack in the box (hitb).* Amsterdam, The Netherlands.

Levillain O. (2012, June 6th). 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.

Observatoire trimestriel des marchés de détail des communications électroniques (services fixes haut et très haut débit) en france - 3e trimestre 2013. (2013). http://www.arcep.fr/index.php ?id=12115.

Proofpoint. (2014, January, 16th). Proofpoint uncovers internet of things (iot) cyberattack. http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799.

Raynal F., Campana G. (2012, October 11th). An attack path to jailbreaking your home router. In *proc. of hack in the box (hitb).* Kuala Lumpur, Malaysia.

Ruff N. (2006, June 1st). Sécurité de l'adsl en france. In *proc. of symposium sur la sécurité des technologies de l'information et des communications (sstic).* Rennes, France.

SIPSorcery. (2012). Sip password security - how much is yours worth? http://www.sipsorcery .com/mainsite/Help/SIPPasswordSecurity.

Vivien. (2011, May 11th). Le retour du combat pppoa / pppoe vs ipoa / ipoe. http://lafibre.info/ techno-du-web/pppoa-pppoe-ipoa-ipoe/.

Wang X., Yu H. (2005, May 23rd). How to break md5 and other hash functions. In *Advances in cryptology–eurocrypt 2005*, p. 19–35. Aarhus, Danmark.