Analyse de sécurité des box ADSL

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

Analyse de sécurité des box ADSL

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

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

Résumé 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. À notre connaissance, relativement peu d'études ont analysé la sécurité de ces BOX ADSL. Cet article présente une méthode innovante d'analyse de sécurité ainsi que des premiers résultats. Nous proposons une méthode permettant d'intercepter et d'analyser tous les protocoles réseaux mis en œuvre lors du démarrage d'une BOX ADSL.

1 Introduction

Le réseau informatique de la majorité des foyers français et d'un grand nombre de PME possède aujourd'hui une BOX ADSL. Ces BOX permettent d'accéder à Internet, mais incluent bien d'autres services tels que la TV ou un point d'accès wifi.

Tout comme pour d'autres équipements informatiques embarqués [2], il est légitime de s'interroger sur la sécurité de ces équipements. L'ANSSI s'inquiète notamment [1] de la possibilité de détourner ces équipements pour constituer un gigantesque réseau de robots informatiques (*botnet*). Plusieurs vulnérabilités ont par ailleurs déjà été identifiées [5,4,3].

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 a donc une très grande liberté d'action ; 2) l'attaquant est sur un site distant et tente d'accéder à la BOX à travers Internet. Un troisième cas de figure doit être pris en compte selon nous, dans lequel l'attaquant opère directement sur la ligne téléphonique reliant l'abonné à l'opérateur. Cet article explore ce troisième cas de figure et propose deux contributions. La première est la conception d'une plateforme permettant 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 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 contribution concerne une seconde plateforme permettant d'émuler le réseau d'un opérateur et ainsi de tirer profit des faiblesses précédemment identifiées.

Cet article est organisé comme suit. La section 2 décrit une plateforme permettant d'écouter le trafic entre une BOX et le fournisseur d'accès à Internet, ainsi que, les résultats de la campagne d'écoute que nous avons menée à l'aide de cette plateforme. Cette expérimentation a permis de mettre 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 3 présente une deuxième plateforme qui nous a permis de montrer qu'il est possible d'exploiter ces vulnérabilités. Enfin, la section 4 propose quelques perspectives à nos travaux.

2 Plateforme d'observation de communications ADSL

Notre premier objectif est 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. Dans un premier temps, nous décrivons notre plateforme dans la sous-section 2.1. Puis, dans un second temps, la sous-section 2.2 est dédiée à la présentation de l'étude comparative que nous avons menée sur la séquence de démarrage des différentes BOX.

2.1 Méthode

L'établissement d'une connexion ADSL nécessite un modem (inclus dans la BOX) et un DSLAM, installé dans les locaux de l'opérateur, à l'autre extrémité de la boucle locale. Ce DSLAM et ce modem, qui sont physiquement reliés par une paire de cuivre, réalisent respectivement l'opération inverse l'un de l'autre. En effet, la modulation utilisée sur la voie montante diffère de celle utilisée sur la voie descendante. C'est pourquoi il est possible de couper physiquement la ligne téléphonique et

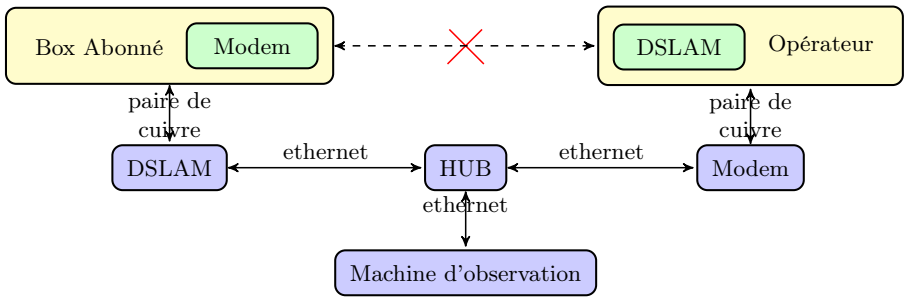

Figure 1. Écoute sur la boucle locale

d'y insérer un DSLAM et un modem ADSL supplémentaire (cf. figure 1), tout en conservant la connectivité entre l'opérateur et l'abonné.

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.

2.2 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.

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.

Les résultats de cette étude sont rassemblés dans le tableau 2. La première colonne contient l'identifiant de la BOX (de manière anonyme). La seconde 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 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.

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	-

Figure 2. Caractéristiques des différentes BOX ADSL déployées en France.

Configuration & mise à jour

La configuration et la mise à jour d'une BOX sont des phases très importantes de la procédure de démarrage. De ce fait, dans la plupart des cas, ces phases utilisent 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 ce fait, si le nom de domaine du serveur contacté contient le terme TR69 (Protocole de gestion de configuration réseau) ou un équivalent, il est raisonnable de supposer que ces échanges concernent la phase de configuration.

Les protocoles utilisés afin de transmettre la configuration et les mises à jours sont présentés respectivement dans l'avant-dernière et dernière colonne du tableau (figure 2). 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. 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.

Cependant, lorsque nous nous intéressons aux BOX *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 1) la configuration lors de leur démarrage et 2) le firmware en cas 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 une méthode itérative afin d'explorer les conséquences de ces faiblesses.

3 Plateforme d'imitation d'un fournisseur d'accès à Internet

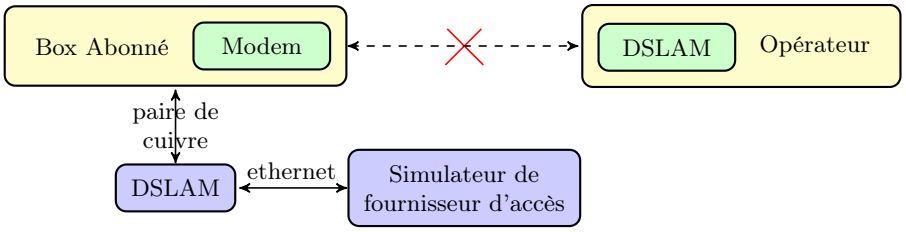

Figure 3. Simulation d'un fournisseur d'accès à Internet

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. Pour cela, 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 3). Nous avons installé et configuré les différents éléments au fur et à mesure en observant le trafic. Nous avons commencé par installer les services PPP et DNS. La réalisation de ces services nous a permis d'atteindre les phases de configuration et de mise à jour de la BOX.

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 et clés privées utilisés. 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 en simulant le serveur de mise à jour du fournisseur d'accès à Internet (FAI). 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 (Wide Area Network) ;
- 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 qui inclura des appels sur-taxés.

4 Conclusion

Des entités étatiques telles que l'ANSSI sont préoccupées par la sécurité des différentes BOX d'aujourd'hui, 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. Dans cet article, nous avons proposé deux méthodes innovantes permettant d'analyser la sécurité de ces équipements d'accès à Internet de nouvelle génération. Il est important de noter que les vulnérabilités identifiées sont difficiles à exploiter et nécessitent des ressources matérielles spécifiques.

Plusieurs contre-mesures aux failles de sécurité identifiées dans cet article, méritent d'être analysées :

- Généralisation de l'utilisation de méthodes cryptographiques lors des phases de configuration.
- Mesure de la variation de l'atténuation du signal sur une ligne ADSL ; cette valeur devrait drastiquement varier lorsqu'une plateforme telle que la nôtre est insérée sur la boucle locale.

En perspective à ces travaux, nous complétons actuellement notre analyse comparative des BOX en France. En effet, nous n'avons pas encore pu analyser toutes les BOX existant aujourd'hui. Une autre perspective sur le long terme est l'analyse d'autres équipements grand public, tels que les téléviseurs et lecteurs Blu-Ray connectés.

Références

1. Défense et sécurité nationale. pages 44–45, Paris, France `http://www.elysee.fr/assets/pdf/Livre-Blanc.pdf`, 2013. Direction de l'information légale et administrive.
2. Ang et al. Cui. When firmware modifications attack. In *proc. of Network and Distributed System Security Symposium (NDSS)*, San Diego, USA, Avril 2008.
3. P. Geissler and S. Ketelaar. How I met your modem. In *proc. of Hack In The Box (HITB)*, Amsterdam, The Netherlands, Avril 2013.
4. F. Raynal and G. Campana. An attack path to jailbreaking your home router. In *proc. of Hack In The Box (HITB)*, Kuala Lumpur, Malaysia, Octobre 2012.
5. 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, Juin 2006.