Sécurité de l'ADSL en France

Nicolas Ruff[1]

EADS-CCR DCR/STI/C
nicolas.ruff@eads.net

1 Introduction

Aujourd'hui l'accès Internet haut débit est devenu courant dans tous les foyers français. La différence entre les opérateurs ne se joue plus sur les tarifs, mais sur la qualité et la richesse des services offerts (support client, téléphonie illimitée, etc.).

Quasiment tous les opérateurs proposent donc aujourd'hui une offre « Triple Play » (Internet / TV / téléphonie) en standard. Pour fonctionner, cette offre nécessite l'acquisition d'une « boite noire » fournie par l'opérateur. Si cette solution satisfait les *end-users* par sa facilité d'installation et de configuration (quoique ...), elle pose légitimement des questions à l'utilisateur averti qui se voit contraint d'abandonner sa passerelle *BSD pour un équipement inconnu.

La sécurité de ces « boites noires » est également une préoccupation bien légitime pour le grand public, aujourd'hui massivement visé par des attaques de toute sorte (installation de bots, phishing/pharming, etc.). L'utilisateur averti ou la PME connectée à l'ADSL se pose des questions sur la possibilité d'utiliser WPA / WPA2 avec ces « boites », la compatibilité du WiFi avec des systèmes d'exploitation non-Microsoft, ou la possibilité d'obtenir un accès *full IP* à Internet.

Cette intervention vise à donner quelques clés permettant à tout un chacun de mesurer les risques liés à l'installation d'une « boite » dans son réseau, et de mieux comprendre le fonctionnement interne de ces équipements.

Le modèle économique retenu pose également d'autres questions, comme :

- La prise en compte de la contrainte d'interception légale sur les communications téléphoniques ;
- La responsabilité légale en cas de problème (ex. modem compromis ayant servi à lancer une attaque).

Ces sujets, quoique passionnants, ne peuvent pas être traités dans une intervention aussi courte qui se concentrera sur les aspects de sécurité informatique uniquement.

2 Sécurité des boites

2.1 Préambule

L'étude présentée ici a été débutée en 2004. Toutefois compte tenu de la sensibilité (commerciale et légale) du sujet, ces travaux n'ont pas pu être présentés au

SSTIC 2005. Heureusement la plupart des problèmes étant aujourd'hui corrigés, il nous est possible de communiquer dessus.

2.2 Hardware

Les boites sont en général basées sur des chipsets « tout-en-un », très souvent de marque Broadcom (ex. BCM 6345, BCM 6410) donc avec un cœur MIPS32. Il est d'ailleurs remarquable de constater que certaines boites vendues par des opérateurs différents sont quasiment identiques au niveau matériel et logiciel ...

A partir de ce constat, on en déduit que :

- Malgré les spécificités du processeur MIPS (architecture « fetch and execute », cache de données et cache d'instructions séparés), l'écriture de *shellcodes* ne posera pas de problème majeur si une faille est découverte.
- Le processeur supporte le débogage de bas niveau via la norme JTAG. Dans les faits, le port JTAG est pratiquement toujours accessible sur la carte mère ; les travaux du projet OpenWRT contiennent tout le nécessaire pour lire et écrire la mémoire Flash via JTAG [OpenWRT].

Outre le port JTAG, la plupart des équipements ont un port série également câblé sur la carte mère, qui permet bien souvent d'obtenir un accès console et/ou de lire les journaux de l'équipement, y compris lors du démarrage. De nombreuses informations utiles s'y trouvent, telles que le chemin d'accès au firmware sur le site du constructeur.

Malgré l'aspect « boite noire » des équipements, leurs secrets ne résistent pas longtemps à un accès physique par leur propriétaire ...

2.3 Système d'exploitation

Les boites se répartissent entre 2 familles au niveau du logiciel embarqué : VxWorks et Linux.

Les boites basées sur VxWorks sont plus difficiles à analyser compte tenu de l'aspect « fermé » du logiciel. Les formats de fichier et les kits de développement ne sont pas publics.

D'un autre côté, le système VxWorks (issu du monde industriel et temps réel) n'a pas été conçu pour être exposé directement à un milieu hostile comme celui d'Internet, et n'offre pas la même richesse logicielle que Linux. Ceci est particulièrement sensible au niveau de :

- La pile IP. En particulier, on notera que les numéros de séquence TCP sont incrémentaux (faille utilisée par Kevin Mitnick pour attaquer Shimomura en ... 1994 !).
- Le serveur Web. Celui-ci se contente de renvoyer une chaine laconique « Server : httpd ». Il s'avère que ce serveur offre un langage de script très limité. Ceci conduit les développeurs à effectuer une grande partie des tâches côté client. En consultant le code source de la page « changement de mot de passe », on trouve par exemple :

```
....
<SCRIPT LANGUAGE=Javascript>
var old_password = "1234";

function CheckPasswd()
 {
  if(document.SubmitChPwdUser.OLDPASSWD.value != old_password)
   {
    .....
```

Les boites basées sur Linux sont faciles à analyser car toutes les documentations et tous les outils de conception sont libres. Certains éditeurs vont jusqu'à respecter la licence GPL en republiant les modifications apportées au code (mais ça n'est pas le cas pour tous).

Les boites basées sur Linux sont souvent mieux armées pour être connectées à Internet et plus riches en fonctionnalités. Mais le nombre de failles découvertes et publiées sur Internet est également plus important, et dans certains cas ces failles s'appliquent aux boites correspondantes (ex. faille ISC DHCP 3.0 [ISC] vs. équipements en mode « routeur »).

2.4 Mise à jour

L'opérateur se doit de pouvoir mettre à jour les équipements pour corriger les failles susmentionnées et proposer des améliorations fonctionnelles. Plusieurs modèles de mise à jour sont utilisés :

- Le mode manuel : l'utilisateur effectue la mise à jour de lui-même, soit en téléchargeant un logiciel exécuté côté client, soit via une option de l'interface de configuration.

Ce mode est obligatoire pour les clients qui sont propriétaires de leur boite, le constructeur ou l'opérateur n'ayant plus le droit d'en changer la configuration. Se pose alors le problème de la non-application des mises à jour, c'est pourquoi la plupart des opérateurs se tournent vers une location de l'équipement. Une partie du parc installé reste et restera néanmoins vulnérable.

- Le mode automatique : l'équipement se met à jour de lui-même depuis un site distant. Cette mise à jour peut souvent être déclenchée par l'utilisateur via l'interface de configuration ou un redémarrage de l'équipement. Cette mise à jour est aussi parfois déclenchée par l'opérateur, ce qui se manifeste par une déconnexion plus ou moins prolongée à un moment aléatoire de la journée (!).

Les mises à jour utilisent le plus souvent le protocole FTP, mais de 2 manières radicalement opposées selon les boites : soit la boite va chercher la mise à jour sur le serveur FTP de l'opérateur, soit le serveur FTP est hébergé sur la boite et l'opérateur vient y poser la mise à jour.

Toutes ces méthodes permettent de récupérer assez facilement les images logicielles qui sont disponibles :

- Soit au téléchargement direct pour une mise à jour manuelle ;

– Soit sur un serveur FTP chez l'opérateur, dont les coordonnées peuvent être trouvées dans une version antérieure du firmware ou dans les journaux d'activité de la console.

Ce sujet ayant été largement couvert dans les forums de bidouille, les liens vers les différentes versions de firmwares sont aujourd'hui accessibles depuis Google. Leur analyse ne pose pas de problème majeur, car les techniques de « brouillage » parfois utilisées restent sommaires et au final il est toujours possible de recomposer l'image CramFS du système Linux (pour les boites sous Linux).

2.5 Interfaces de configuration

Quasiment toutes les boites possèdent une adresse IP côté LAN. Même une boite ne possédant qu'un seul port Ethernet et ne supportant pas a priori de mode « routeur » écoute malgré tout sur une adresse IP RFC 1918 qui permet d'accéder à l'interface de configuration.

Les ports TCP ouverts sont en général toujours les mêmes : FTP/21, Telnet/23, Web/80 (et parfois SSH/22).

Les comptes prédéfinis dans l'équipement sont nombreux, rarement moins de 4 : un compte utilisateur (documenté), un compte de support dont le mot de passe est parfois divulgué par le support technique, un compte opérateur et un compte constructeur.

Le compte utilisateur possède toujours un mot de passe trivial et très bien documenté sur Internet. Malgré les recommandations de la documentation, un sondage rapide auprès de quelques amis internautes montre que ce mot de passe n'est *jamais* changé.

Les comptes de support de quelques opérateurs sont également documentés sur Internet.

Enfin le compte 'root', présent aussi bien sur des équipements Linux que VxWorks, possède le mot de passe '1234' chez un opérateur et '12345' chez un autre. Là encore l'information a fini par fuir sur Internet.

Le service FTP est souvent accessible à l'utilisateur *anonymous*, en plus des comptes susmentionnés. Selon les configurations, l'énumération des fichiers est possible ou non. Mais dans tous les cas il est possible de récupérer le firmware sous réserve de connaître le nom de fichier complet, voire d'écrire un nouveau firmware sous réserve de comprendre l'algorithme de *checksum* (et non de signature) utilisé.

Le service Web de configuration n'est pas toujours authentifié, de plus les limitations des serveurs utilisés (principalement sous VxWorks) les rendent vulnérables à des attaques triviales. Sur un équipement, il est par exemple possible de récupérer toute la configuration en se rendant à l'URL "http ://<ip privée>/config/", y compris la liste des comptes et mots de passe en clair.

Notons que l'option d'archivage de la configuration, présente sur un grand nombre d'équipements, est susceptible de représenter une faille importante. En effet il est non seulement possible de récupérer des informations normalement inaccessibles depuis l'interface de configuration (comme la liste des comptes et

mots de passe), mais il est également possible de modifier ces paramètres lors de la restauration.

Pour mesurer toute l'ampleur de cette attaque, il ne faut pas oublier que sous Linux ces fichiers de configuration sont le plus souvent directement inclus dans des scripts de démarrage ...

Il a également été constaté que toutes les interfaces Web renvoient les véritables informations d'authentification derrière les astérisques des champs « mots de passe ». Il est donc possible de retrouver ses mots de passe, clés WEP, etc. dans le code source des pages Web d'administration.

Enfin le service Telnet offre souvent des commandes intéressantes, en particulier sous VxWorks où des commandes telles que *mread* (*memory read*), *mwrite* (*memory write*), ou *debug* sont parfois laissées actives. Il faut noter que ces commandes n'apparaissent pas toujours dans la sortie de la commande *help*.

2.6 WiFi

La plupart des boites possèdent une option WiFi, sous forme de carte PCMCIA additionnelle. Les technologies d'accès WiFi sont très variables d'un opérateur à l'autre. On citera les configurations suivantes :

- Absence de WEP/WPA et utilisation d'une technologie « PPP over WiFi ». Cette technologie possède tous les inconvénients : impossibilité de partager la connexion WiFi entre plusieurs clients, écoute du trafic par des tiers, capture des authentifiants.
- WEP. Souvent la seule solution offerte aux clients jusqu'à l'année dernière, malheureusement l'insécurité du WEP n'est plus à démontrer aujourd'hui.
- WEP + technologie propriétaire de rotation de clés. Plus sécurisée que la solution précédente, cette solution est en pratique inacceptable pour les clients : nécessité d'acheter un dongle USB propriétaire pour chaque machine, absence de drivers pour Linux, MacOS et autres gadgets WiFi (PDAs, appareils photos, Nabaztags, etc.). De plus l'algorithme de rotation des clés n'ayant pas fait l'objet d'études publiques, on pourrait douter de sa solidité cryptographique.
- WPA. La meilleure solution disponible, à condition de choisir une passphrase suffisamment forte. Malheureusement l'expérience prouve que la plupart des clients sont restés en WEP même après l'intégration de WPA dans les firmwares. De plus la passphrase WPA par défaut est identique à l'ancienne clé WEP ...

Chez certains opérateurs, d'autres astuces sont utilisées pour limiter la casse au niveau WiFi, telles que la nécessité d'une action matérielle pour associer de nouvelles cartes (bouton poussoir). Malheureusement, les cartes en question étant identifiées par leur adresse MAC, cette protection empêche simplement la connexion simultanée d'un client et d'un pirate ... (et encore).

Un dernier point resté totalement mystérieux est la possibilité pour le constructeur de valider une association entre une clé WEP et le numéro de série de l'équipement (basé sur son adresse MAC). Ces informations sont utilisées pour se connecter au site Web de support par exemple. Il n'a pas pu être déterminé

s'il existait un algorithme de dérivation adresse MAC -> clé WEP, ou si l'ensemble des clés WEP par défaut sur chaque borne vendue étaient stockées dans une base.

En conclusion on peut noter que le WiFi est un véritable point faible sur les équipements non-WPA. Ce point est particulièrement inquiétant quand on connaît les faiblesses des interfaces d'administration vues précédemment : l'accès à une boite permet par exemple de retrouver les identifiants de connexion ou d'activer des services. Certains services sont ensuite imputés directement sur la facture du possesseur de la boite ...

2.7 Bluetooth

Un court paragraphe sur le Bluetooth, peu d'équipements en étant dotés.

Le code PIN par défaut utilisé pour l'association de nouveaux équipements est trivial (ex. 0000 ou 1234). Une association Bluetooth réussie permet un accès complet à la boite, identique à celui obtenu par lien filaire ou WiFi. Quand on sait que des liaisons Bluetooth ont été établies à plus de 1,5 km par le groupe Trifinite [Trifinite] (avec le matériel adéquat), il y aurait lieu de s'inquiéter.

Heureusement l'ajout d'un élément matériel nécessaire à l'association (bouton poussoir) rend les attaques beaucoup plus complexes. Le protocole BlueTooth étant plus sûr par conception que le WiFi, l'usurpation d'adresse MAC ne suffit pas à pouvoir établir une connexion.

3 Sécurité de l'infrastructure

3.1 Préambule

Les opérateurs se trouvent dans une configuration beaucoup plus hostile que la plupart des réseaux d'entreprise : ils doivent non seulement faire face aux attaques provenant d'Internet, mais également aux attaques et aux tentatives de fraude provenant de l'intérieur de leur réseau, le tout avec un nombre de clients dépassant largement les plus gros LAN d'entreprise (jusqu'à plusieurs millions).

On peut donc imaginer que les problématiques de détection d'intrusion et de supervision sont décuplées par rapport à la moyenne de l'industrie.

Toutefois les opérateurs communiquent peu sur le sujet, et il est assez délicat d'effectuer des tests « en aveugle ». Les résultats ci-dessous présentent une vue générale et les risques potentiels des réseaux explorés.

3.2 Circuits ATM

Les réseaux d'opérateurs sont bien souvent basés sur ATM dès la sortie de la boite. Sans trop rentrer dans les détails du protocole [ATM], disons simplement qu'une cellule ATM se compose de 48 octets de données et 5 octets d'en-tête. Cet entête comprend un *Virtual Circuit Identifier* (VCI) sur 16 bits

et un *Virtual Path Identifier* (VPI) sur 8 ou 12 bits qui à eux deux identifient un canal ATM.

La plupart des réseaux de transport de données utilisent le VCI/VPI 8/35 ou 8/36. Les interfaces de configuration permettent parfois d'avoir accès aux paramètres ATM utilisés pour les autres réseaux (téléphonie, TV) – dans la majorité des cas les paramètres VCI/VPI sont compris entre 8/35 et 8/50.

Explorer les canaux ATM nécessite un modem ADSL autorisant un réglage VCI/VPI manuel, c'est-à-dire n'importe quel modem du commerce autre qu'une « boite » opérateur.

Il apparaît alors assez rapidement que la majorité des canaux ATM utilisés transportent de l'IP et offrent tous les services classiques sur un réseau IP, comme le DHCP. Certains canaux sont probablement utilisés par les opérateurs pour la télémaintenance et la mise à jour des équipements, le serveur DHCP renvoyant une adresse privée RFC 1918. Sur ces canaux, les communications inter-boites sont relativement peu filtrées ...

3.3 Serveurs de mise à jour

Les serveurs de mise à jour (contenant les images de firmwares) sont des nœuds essentiels du réseau : en cas de compromission, on comprend que les conséquences puissent être assez graves.

Malgré la sensibilité de ces serveurs, tous ne suivent pas les « meilleures pratiques » en termes de sécurité. On rencontre bien souvent des serveurs partageant les mêmes répertoires en HTTP et FTP. Or si un attaquant réussit à déposer un fichier PHP via FTP, puis à y accéder via HTTP, le serveur est compromis. D'autres erreurs de configuration sont présentes, telles que : accès aux fichiers « .htaccess » et « .htpasswd » via FTP, énumération des répertoires possible via HTTP, etc.

3.4 Autres serveurs

D'autres serveurs sont particulièrement sensibles, compte tenu de la nature commerciale des services qu'ils hébergent : ce sont les serveurs de *streaming* TV et les serveurs de VoIP.

Le sujet est toutefois trop sensible pour être traité dans une conférence grand public.

4 Conclusion

4.1 Synthèse des résultats

En imposant l'utilisation d'un modem unique, propriétaire, à leurs clients, les principaux opérateurs d'accès Internet s'imposent la lourde tâche de veiller à la sécurité de ces « boites », qui méritent bien le titre de « boites noires » ... même si certaines arborent des couleurs *fashion*.

Le risque auquel les opérateurs se confrontent est grand, car la diminution de la diversité augmente la potentialité et l'étendue d'une attaque. De plus les gains financiers possibles, liés aux services payants, renforcent l'intérêt de telles attaques.

Or la plupart des « boites » souffrent d'erreurs de conception en terme de sécurité, la plus critique étant l'utilisation de mots de passe simples et universels pour accéder à la configuration complète de l'équipement (ces mots de passe n'étant pas tous documentés et modifiables par les utilisateurs).

Dès lors il est possible d'envisager de multiples scénarios, détaillés ci-après.

En cas de problème grave se posera inévitablement la question des responsabilités, entre l'opérateur, le constructeur et le client ; d'autant que certains équipements sont loués, d'autres prêtés et d'autres encore vendus (échappant légalement à tout contrôle de l'opérateur). De plus les capacités de journalisation des boites étant limitées voire nulles, les investigations techniques s'avèreront probablement impossible. Cela augure de procès complexes à venir ...

4.2 Scénarios

Sans vouloir donner trop d'idées aux malfaisants, on imagine assez bien quelques scénarios parfaitement crédibles sur la base de l'étude précédente.

L'installation d'un module logiciel sur les boites est une première étape. Ce module pourra avoir des fonctions à la mode telles que :

- Servir de bot pour un DDoS ;
- Servir de relais de spam ;
- Ecouter toutes les communications sur le lien ADSL pour capturer des mots de passe ou du trafic HTTP. Contrairement aux attaques du poste client, les communications SSL sont protégées contre l'écoute, mais pas les protocoles de type POP3 (utilisé par quasiment tous les hébergeurs).

Ce module peut être installé :

- Soit par un virus se propageant côté client ;
- Soit par une interface d'administration accessible côté ADSL, éventuellement sur un canal ATM particulier ;
- Soit par un serveur de firmware compromis.

A ce point, si le module hostile désactive les fonctions de mise à jour automatique et change les mots de passe par défaut, seul une intervention physique opérée par le constructeur permettrait de reprendre le contrôle de l'équipement.

On peut également envisager la propagation d'un virus capable de bloquer toutes les boites. La non-propagation d'un tel virus, ou l'accès aux nouveaux mots de passe installés par le virus, se monnaierait probablement assez cher pour l'opérateur.

Enfin on peut également citer les attaques auxquelles tout le monde pense, à savoir :

- Redirection du trafic téléphonique pour interception ;
- Contournement des systèmes de facturation téléphonie/télévision.

La faisabilité de telles attaques reste plus difficile à évaluer.

Bref, compte tenu des gains potentiels pour les attaquants, il est presque surprenant qu'aucune attaque n'ait encore eu lieu ...

Remerciements

Je remercie toute l'équipe DCR/STI/C du Centre de Recherche EADS pour sa compétence et son soutien logistique.

Références

[OpenWRT] OpenWRT Debrick utility, `http://downloads.openwrt.org/utils/`

[ISC] Faille ISC DHCP 3.0, `http://secunia.com/advisories/11923/`

[Trifinite] Trifinite, `http://www.trifinite.org/`

[BSS] Bluetooth Stack Smasher (BSS), `http://securitech.homeunix.org/blue/`

[ATM] Wikipédia : le protocole ATM, `http://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode`