

# WiFi, Présumé coupable

Olivier "*Bluetouff*" Laurelli  
BEARSTECH

21 juin 2010



# Table des matières

<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	Le délit de négligence caractérisée . . . . .	6
1.1.1	Le contexte . . . . .	6
1.1.2	Un premier constat, évident comme le nez au milieu de la figure . . . . .	6
1.2	Que veut dire sécuriser une connexion Internet ? . . . . .	7
1.2.1	Qui peut être tenu responsable de quoi ? . . . . .	7
1.2.2	On récapitule . . . . .	9
1.2.3	Riposte graduée, législateur sourd : justice aveugle ? . . . . .	9
1.2.4	Les faiblesses du poste de travail . . . . .	10
<b>2</b>	<b>Le WiFi : la menace fantôme</b>	<b>11</b>
2.1	Une technologie adoptée massivement . . . . .	11
2.2	Les réseaux sans fil et le chiffrement . . . . .	12
2.3	WPA, WPA2, PSK, TKIP et AES . . . . .	12
2.4	Le mode Ad-Hoc . . . . .	14
<b>3</b>	<b>Les pratiques des FAI en matière de sécurité WiFi</b>	<b>15</b>
3.1	La Bbox . . . . .	15
3.2	Numéricable . . . . .	15
3.3	Freebox . . . . .	16
3.4	Combien Hadopi va t-elle coûter à l'opérateur ? . . . . .	17
<b>4</b>	<b>Le WiFi dans les lieux publics</b>	<b>18</b>
<b>5</b>	<b>Démonstrations</b>	<b>20</b>
5.1	Routeur - réseaux payants . . . . .	20
5.2	Les pratiques des entreprises . . . . .	23
<b>6</b>	<b>Conclusion</b>	<b>24</b>



# Chapitre 1

## Introduction

### 1.1 Le délit de négligence caractérisée

#### 1.1.1 Le contexte

Le délit de négligence caractérisée, tel que défini par la loi Création et Internet<sup>1</sup>, dite loi *Hadopi*<sup>2</sup>, vise à rendre chaque utilisateur d'internet responsable de la sécurité de son installation informatique. C'est une nouveauté législative qu'il convient de définir comme étant dangereuse, car seule une infime minorité d'internautes, en France comme dans le monde, sont aptes à comprendre et à maîtriser les bases de la sécurité des communications sur Internet.

#### 1.1.2 Un premier constat, évident comme le nez au milieu de la figure

Hadopi n'est pas tombée du ciel, et son cortège de mesures techniques, qu'il s'agisse du filtrage, du « logiciel de sécurisation » (un logiciel espion prévu dans la loi, seule solution pour bénéficier d'une présomption d'innocence), ou encore des listes blanches sur les réseaux WiFi publics, ne sont pas l'oeuvre de Christine Albanel<sup>3</sup> ou de Olivier Henrard, son conseiller. Le CGTI<sup>4</sup>, dans un rapport<sup>5</sup> rédigé pour le Ministère de la Culture a guidé sa réflexion, et la loi qui en a résulté reflète l'incompréhension totale de ce dernier. Cette incompréhension va avoir dans les mois qui viennent des conséquences inattendues par le législateur, et vous allez vite comprendre à la lecture de ce qui suit que personne n'a réfléchi sérieusement aux conséquences de cette loi. Hadopi est une loi inapplicable, coûteuse, et qui crée des injustices. Nous ne serons pas tous égaux devant Hadopi, les techniciens et les plus aisés d'entre nous seront bien plus égaux que les autres. Les ordonnances pénales prévues par le texte de loi aboutiront dans de nombreux cas à de coûteuses procédures : soit vous aurez les moyens financiers et techniques de vous défendre, soit vous risquez d'en être victime, accusé à tort, sans être en mesure de prouver votre bonne foi.

---

<sup>1</sup>Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création

<sup>2</sup>Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet

<sup>3</sup>Ministre de la Culture et de la Communication en France (2007 à 2009)

<sup>4</sup>Conseil Général des Technologies de l'Information

<sup>5</sup>disponible par exemple ici : <http://www.lesechos.fr/medias/2009/0304//300333937.pdf>

## 1.2 Que veut dire sécuriser une connexion Internet ?

Contrairement à ce que laissent entendre ces mots, la sécurité des communications sur Internet ne peut se restreindre au tuyau ou à la ligne téléphonique sensée acheminer vos communications. Une connexion s'établit à partir d'un ordinateur, qui demande au modem d'accéder à Internet pour envoyer des "paquets" dans un tuyau (câble, ADSL, ou fibre optique), vers un serveur. Le serveur ainsi contacté vous répond : la connexion est alors établie.

Nous venons ainsi d'identifier 3 maillons de la chaîne (il y en a en fait bien plus et tous présentent des risques plus ou moins élevés) :

- l'ordinateur
- le modem
- le serveur distant

Sécuriser une connexion signifie que chacun de ces maillons est "sécurisé". Si l'internaute a généralement le contrôle de son propre ordinateur, il peut paraître curieux que la loi lui impose de sécuriser 2 autres de ces maillons, qu'il ne contrôle pas. Quand bien même il souhaiterait le faire, seul une poignée d'internautes dispose des compétences nécessaires en administration réseaux pour y parvenir. Pour les autres, soit 99%, il leur faudrait suivre une formation de plusieurs années.

### 1.2.1 Qui peut être tenu responsable de quoi ?

#### Constat numéro 1 :

Peu d'internautes comprennent comment le système d'exploitation de leur ordinateur fonctionne, seul un tout petit public d'ingénieurs ou de professionnels de l'informatique peut se targuer de parfaitement comprendre ce qui rentre et sort de son ordinateur (c'est pourtant cela que la Hadopi lui demande de surveiller).

Les systèmes d'exploitation "propriétaires"<sup>6</sup> comme Windows ou MacOSX, soit environ 99% de ceux utilisés par les particuliers, font d'ailleurs tout ce qu'ils peuvent pour ajouter des "couches d'abstraction" supplémentaires et faire en sorte que l'utilisateur trouve cela « magique » et ne s'en soucie guère.

L'informatique est quelque chose de complexe, il est normal de simplifier les choses le plus possible afin que l'utilisateur puisse se concentrer sur ses tâches, sans avoir à se soucier de la façon dont ces dernières sont traitées techniquement.

Ce raisonnement ne choquera personne, mais en matière de sécurité, rien n'est magique, et l'histoire ne cesse de nous démontrer que la sécurité par l'obscurantisme ne fonctionne pas, mais alors pas du tout. Or c'est malheureusement la posture adoptée par de trop nombreux éditeurs logiciels.

Ainsi, on a appris l'année dernière que Microsoft avait corrigé dans sa suite

---

<sup>6</sup>par opposition à des systèmes "open-source" comme Gnu/Linux

MS Office une faille vieille de plus de sept ans, présentée en 2000 lors de la plus importante convention mondiale de hackers « blackhats<sup>7</sup> » se tenant chaque année à Las Vegas, le Defcon<sup>8</sup> (c'est dire si la faille n'était pas confidentielle). Une autre vulnérabilité, très critique, dans le noyau XML maison, aura dû attendre deux ans pour que Microsoft ne daigne se pencher dessus.

Les logiciels libres ne sont pas non plus irréprochables, d'une manière générale, des choix de développement peuvent inciter les développeur à ne pas réparer un trou de sécurité, ce n'est pas parce que le code est disponible publiquement qu'il est exempt de défaut et que ses utilisateurs vont le "patcher" eux même.

En clair, les logiciels que vous utilisez tous les jours sont truffés de trous de sécurité, et même ceux qui les construisent ne sont pas en mesure d'assurer une sécurité sans faille.

### **Constat numéro 2 :**

Les « box », composants central des offres "triple play" si courantes en France, sont une plaie. Ce sont des boites noires dans lesquelles il est impossible, pour le commun des mortels, de savoir ce qu'il s'y passe, et parfois, c'est pas beau à voir, nous y reviendrons un peu plus loin.

A ce jour, chez les grands opérateurs internet, seul Neuf Télécom permet à ses utilisateurs un niveau de contrôle satisfaisant, en fournissant les sources du firmware<sup>9</sup> de sa NeufBox, et permettant son remplacement par des firmwares alternatifs. Orange s'est réveillé récemment, curieusement, et a enfin publié ses sources (après des années de résistance et des trésors de mauvaise foi affichés face à la grogne de certains utilisateurs sur feu le site web du Orange Lab).

Le mauvais élève de la classe, Free, persiste à ne pas libérer le code de sa Freebox, violant ainsi la licence GPL<sup>10</sup> (General Public Licence) des nombreux logiciels qu'il utilise.

En pratique, la première source d'insécurité d'une connexion Internet, après l'ordinateur du particulier, sont les "box" et les modems. Une vulnérabilité exploitable à distance sur une Livebox d'Orange a d'ailleurs déjà été révélée.

### **Constat numéro 3 :**

"Il n'existe pas de patch contre la stupidité et l'ignorance", et cela les éditeurs d'antivirus le savent bien. Pour certain, c'est même un fond de commerce intarissable.

---

<sup>7</sup>De façon très réductrice, on distingue les "gentil" hacker (Whitehat) et les "méchants" (Blackhat).

<sup>8</sup><http://www.defcon.org/>

<sup>9</sup>Firmware : système d'exploitation embarqué basé sur GNU/Linux, nécessaire pour faire fonctionner les services qui tournent sur cette Box.

<sup>10</sup>Free argue du fait que la licence GPL stipule que la redistribution du code est obligatoire dans le cadre d'une distribution des équipement et que comme la Freebox est mise à disposition des Freenaute en restant la propriété de Free, le code source n'a pas à être révélé... une interprétation originale de la GPL selon la Free Software Foundation et de nombreux développeurs ou utilisateurs de logiciels libres.

Abuser de la faiblesse et des lacune techniques des utilisateurs est une entreprise très lucrative. Si on ajoute à cette psychose la peur du gendarme en brandissant le spectre d'une coupure d'Internet, il faut s'attendre à voir fleurir sur le marché de nombreuses solutions « miracles », qui vont vous garantir la « sécurité absolue pour 5 euros par mois ». Les fournisseurs d'accès les y aideront et prendront leur petite commission au passage.

#### **Constat numéro 4 :**

On attend toujours les spécifications du "logiciel de sécurisation" , que Christine Albanel assimilait par on ne sait trop quel merveilleux raisonnement à la suite bureautique libre OpenOffice.

Avec ce genre de fondation, allez savoir pourquoi l'édifice nous semble bancal...

#### **1.2.2 On récapitule**

- Les éditeurs logiciels propriétaires n'autorisent pas les utilisateurs à bénéficier du droit de contrôle nécessaire à une bonne sécurisation de leur système. Pire, ces éditeurs sont eux mêmes coupables d'une certaine négligence (caractérisée, ou non) quand ils rechignent à fournir les correctifs nécessaires, et il peut se passer plusieurs années avant qu'il ne daignent apporter une réponse à une faille de sécurité connu de tous les spécialistes.
- Les opérateurs, et certains fabricants d'équipements réseaux (modems/routeurs), suivent le modèle des éditeurs logiciels propriétaires.
- L'opacité générée par les deux points précédents est facilement exploitable, et va créer un business nauséabond, qui confinera les utilisateurs dans une profonde et lucrative ignorance.

De toutes évidence, les personnes qui ont défendu le texte Création et Internet n'ont pas compris grand chose à ces trois points.

#### **1.2.3 Riposte graduée, législateur sourd : justice aveugle ?**

Un utilisateur peut-il assumer la responsabilité juridiques d'erreurs techniques qui ne sont pas de son fait ? C'est bien là une question à se poser. Certains députés<sup>11</sup> s'en sont d'ailleurs fait l'écho, même si ces mêmes députés ont par deux fois voté le texte Création et Internet. Les décrets d'application du texte de loi Création et Internet vont devoir répondre à des problématiques complexes, que le ministère de la Culture était bien loin d'envisager. Sa lecture de l'avis de CGTI et le texte qui en a été extrait montre que manifestement, la rue de Valois ne maîtrisait pas son sujet et a préféré occulter le plus possible ces « points de détails » techniques, qui ne tromperont pas les juges.

Peut on déceimment condamner une personne pour un délit de négligence caractérisée, alors qu'elle n'a pas les moyens techniques de se prémunir des risques, et qu'elle n'est elle même pas l'auteur de la négligence en question ?

---

<sup>11</sup><http://www.pcinpact.com/actu/news/54271-franois-loos-vote-Hadopi-securisation.htm>

### 1.2.4 Les faiblesses du poste de travail

Combien de temps un internaute moyen passe-t-il chaque semaine à faire la chasse aux malwares, virus, rootkits et adwares en tout genre qui pullulent sur Internet ? Certains spécialistes dont Vincent Cerf, l'un des père fondateur de l'internet, affirment que plus d'un quart du parc mondial est infecté, et présente dès lors d'importantes vulnérabilités permettant une prise de contrôle à distance par des tiers.

C'est d'ailleurs le seul point sur lequel on peut s'estimer d'accord avec la récente paranoïa du député Myard<sup>12</sup>, qui propose de nationaliser Internet car des « chevaux de Troie peuvent se réveiller demain matin ». Le député commet cependant une erreur de base, qui ne fait que lever le voile sur l'incompétence manifeste du législateur sur ces problématiques. Nationaliser Internet ne préservera en rien ses utilisateurs des failles inhérentes à leurs systèmes d'exploitation, aux logiciels qu'ils utilisent, auquel on ajoutera les risques de vol d'information sur le réseaux sociaux qui peuvent avoir des conséquences lourdes, directes et très perceptibles comme nous allons le voir un peu plus loin avec les mots de passe de réseaux wifi.

On pourra s'étonner, au passage, du manque de cohérence du député Myard, qui bien que conscient de ces failles de sécurité, a voté pour Hadopi et son délit de négligence caractérisée.

---

<sup>12</sup><http://blog.fdn.fr/post/2009/12/18/Il-faut-répondre-à-Jacques-Myard>

## Chapitre 2

# Le WiFi : la menace fantôme

### 2.1 Une technologie adoptée massivement

Les technologies d'accès à l'Internet sans fil ont vraiment révolutionné les usages des internautes. Largement adoptées, elles permettent à de nombreux utilisateurs nomades d'accéder à Internet alors qu'ils sont en déplacement.

Le WiFi est plébiscité dans la sphère privée, or le WiFi, c'est avant tout des ondes et celles-ci ne s'arrêtent pas à la porte de votre domicile. Votre réseau est visible et théoriquement accessible de l'extérieur, sans qu'aucun contact physique ne soit nécessaire avec vos équipements. Avec une antenne adapté, un réseau peut être accessible à plusieurs kilomètres de distance.

Derrière la magie du WiFi se cache également une réalité peu flatteuse : de nombreuses carences en matière de sécurité. Protocoles de chiffrement obsolètes, mauvaises implémentations des protocoles de la part des constructeurs : l'utilisateur, généralement peu au fait des protocoles de chiffrement et les problématiques de sécurité, peut rapidement se retrouver victime de son manque d'expertise, et n'a même pas, dans la majorité des cas, les compétences techniques pour les comprendre.

Si nous sommes tous en théorie égaux devant la loi, nous le sommes généralement beaucoup moins devant la technologie.

De nos jours, le WiFi est intégré à toutes les "box" comprises dans les offres des grands opérateurs. Pas un ordinateur portable vendu aujourd'hui dans le commerce n'en est dépourvu. Le WiFi est partout, utilisé par des millions de français quotidiennement. S'il présente un aspect pratique indéniable, le WiFi pose cependant de nombreux problèmes de sécurité. Le premier de ces problèmes vient du fait qu'il nécessite pas de liaison physique (pas de câble), et qu'il est visible à des distances relativement importante, presque toujours hors de la maison ou de l'appartement dans lequel se trouve le point d'accès à internet. Une personne malveillante connectée à votre réseau WiFi est en mesure d'intercepter le trafic qui y circule, tout comme il le ferait sur un réseau local filaire.

Les outils d'interception ne manquent pas (Dsniff, Wireshark, Mailsnarf...) : mails, trafic web, mots de passes, tout peut être intercepté relativement facilement.

## 2.2 Les réseaux sans fil et le chiffrement

Pour pallier ce problème et ne pas offrir vos données à vos voisins, les constructeurs ont très rapidement implémenté des protocoles de chiffrement des communications et d'authentification. Le plus ancien d'entre eux, encore très largement répandu, se nomme WEP (Wired Equivalent Privacy) et se décline en 3 versions correspondant à une taille des clés de chiffrement : 64, 128 et 256 bits (ce dernier est beaucoup plus rare). Le WEP a deux faiblesses bien connues :

- Le principe de clef partagée<sup>1</sup> : Le point d'accès et votre ordinateur partagent la même clef.
- Les vecteurs d'initialisation : dans l'exemple d'un chiffrement en 128 bits, seuls les 104 qui composent la clef RC4 (un algorithme de chiffrement) sont effectivement chiffrés. Ceci veut dire que 24 bits passent en clair, ces bits se nomment IV, ou vecteurs d'initialisation.

Pour exploiter les faiblesses du WEP, il suffit donc d'écouter ce qui se passe sur le réseau, d'intercepter un nombre suffisant de paquets qui passent en clair (les IV), et d'en extrapoler les bits restants pour en déduire la clef de chiffrement. Cette opération peut être relativement longue, mais il suffit de s'équiper du bon matériel<sup>2</sup> pour être en mesure d'injecter des paquets et de générer un trafic artificiel qui vous permettra d'obtenir la clef de chiffrement du réseau cible en quelques minutes (là où plusieurs jours seraient nécessaires en ne pratiquant qu'une simple écoute passive).

Le WEP n'est donc pas un protocole que l'on peut sérieusement considérer comme étant sécurisé, de nombreux outils existent pour en venir relativement facilement à bout, comme Aircrack-ng, Kismet ou Kismet.

## 2.3 WPA, WPA2, PSK, TKIP et AES

Le WEP n'étant pas du tout fiable, il a fallu répondre à ses faiblesses. Le WPA (WiFi Protected Access) a donc fait son apparition. Il faut noter que le WPA est un protocole de transition, en prévision du 802.11i, implémenté par le WPA2. Le WPA est un protocole basé sur son ancêtre, le WEP, sur lequel on a ajouté une couche supplémentaire : le TKIP. Le TKIP ajoute au paquet WEP un code MAC pour authentifier les messages.

En 2008, Éric Tews et Martin Beck, deux chercheurs allemands, ont trouvé le moyen d'extraire le code MAC des paquets WEP, et ainsi, de se faire passer pour le point d'accès. Il s'agit d'une attaque MITM (Man In the Middle) de la couche TKIP, le WPA lui-même n'a pas été cracké comme a pu souvent le lire dans la presse (les médias sont loin de comprendre ces mécanismes). Le TKIP,

---

<sup>1</sup>on parle de chiffrement symétrique, connu pour être moins coûteux en terme de ressources qu'un chiffrement asymétrique.

<sup>2</sup>[http://www.aircrack-ng.org/doku.php?id=compatibility\\_drivers](http://www.aircrack-ng.org/doku.php?id=compatibility_drivers)

en revanche, a largement montré ses limites.

Le WPA/TKIP est à ce jour la méthode de chiffrement des réseaux sans fil la plus utilisée en France, et comme nous venons de le voir, elle est faillible. Le WPA2 ou la norme 802.11i implémente le chiffrement AES. Petit point de détail, de nombreux matériels anciens (de plus de 5 ans) sont incompatibles avec cette norme, ce qui veut donc dire que si vous possédez un matériel un peu ancien, il va falloir en changer pour espérer être en conformité avec les bonnes pratiques de sécurisation du WiFi.

Pour comprendre les limites du WPA2 il faut gratter du côté du PSK, ou le mode Pre-Shared Key. On peut lire sur de nombreux sites web que le WPA2 est sécurisé et que le WPA ne l'est pas : tout cela est faux, ils ont en fait une faiblesse partagée : le PSK, communément appelé le mode « Personal », choix par défaut de l'immense majorité des équipements WiFi des opérateurs comme des constructeurs.

Le PSK est vulnérable à des attaques par force brute, qui consistent à utiliser des dictionnaires de mot de passe, de simples listes de mots, et de les faire défiler jusqu'à ce que l'on tombe sur le bon. Certes, cette opération peut être longue, et infructueuse, si la cible a choisi un mot de passe composé d'un nombre suffisant de caractères et ne risquant pas de se trouver dans un dictionnaire (une suite de caractères alphanumériques avec des caractères spéciaux est très vivement recommandée).

Mais de nos jours, les cartes graphiques ne servent pas seulement à faire tourner les derniers jeux en 3D à la mode. Les GPU<sup>3</sup> sont d'une puissance telle qu'elles peuvent être utilisées pour réaliser ce type d'opération grâce aux technologies OpenCL ou Cuda et faire économiser de longues heures (et même des jours entiers) à l'assaillant. Ajoutez à cela la technologie SLI qui permet de paralléliser la puissance de calcul de plusieurs cartes graphiques, et vous obtenez une insécurité sans cesse croissante.

WPA-PSK ou WPA2-PSK (WPA Personal et WPA2 Personal comme nous avons l'habitude de les voir appelés) sont donc faillibles eux aussi. Il existe même des services en ligne vous permettant de louer un cloud<sup>4</sup> pour casser du WPA ! Mais alors que nous reste t-il pour nous protéger convenablement ?

- 1. Si vous n'avez rien compris à ce qui est écrit ci-dessus et que vous souhaitez être protégés : éteignez tous vos équipements WiFi.
- 2. Si vous avez compris ce qui est écrit ci-dessus mais que vous n'avez pas un niveau technique ni les fonds nécessaires vous permettant de déployer une coûteuse solution professionnelle, vous prendrez soin d'observer les règles suivantes :
  - a. Au pire, choisissez le mode WPA ou WPA2 Personal (de préférence WPA2 Personal), mais en aucun cas le WEP ;
  - b. Au mieux choisissez du WPA2/CCMP/AES

---

<sup>3</sup>GPU : Graphic Processeur Unit ou processeurs graphiques.

<sup>4</sup><http://bluetouff.com/2009/12/09/contourner-Hadopi-pour-les-nuls-partie-17-faites-accuser-votrevoisin>

- c. Générez une passphrase ou une suite de caractères assez longue avec des caractères spéciaux qui ne risque pas de se retrouver dans un dictionnaire ou trop rapidement de manière incrémentale;
  - d. Changez régulièrement cette passphrase.
- 3. Si vous êtes une entreprise ou une personne fortunée qui ne peut pas se passer du WiFi, préférez le mode WPA ou WPA2 Entreprise et une authentification renforcée EAP (Extensible Authentication Protocol), cela coûte plus cher à mettre en place, c'est loin d'être à la portée de tout le monde et supporté par tous les matériels (gestion de certificats, mise en place d'un serveur Radius...), mais c'est une bonne méthode pour avoir la paix.

## 2.4 Le mode Ad-Hoc

Dans un lieu public comme une gare, un hôtel, dans le train ou l'avion... il y a toujours ce que l'on appelle de « bons clients » : une personne qui a laissé son ordinateur avec le WiFi allumé en mode Ad-Hoc, avec un partage de fichiers bien visible et accessible.

N'importe qui peut s'y connecter et ainsi récupérer les documents présents dans son dossier partagé, et parfois bien plus. Windows ne vous force pas à mettre de mot de passe sur un compte administrateur et ce seul point est responsable de nombreuses intrusions et de fuites d'informations. Ce fait combiné à un partage de fichiers mal configuré rendra l'intégralité de votre disque dur accessible à une personne mal intentionnée. Ajoutez à cela que les machines configurées de la sorte sont souvent des ordinateurs d'entreprises, remplies de documents relativement confidentiels...

## Chapitre 3

# Les pratiques des FAI en matière de sécurité WiFi

Les anciennes et encore très nombreuses anciennes box de ces FAI proposent par défaut du WEP, les nouvelles proposent maintenant du WPA. Aucun de ces fournisseur d'accès n'a pour le moment jugé bon d'informer le public des risques du WEP comme réglage par défaut sur ses box.

### 3.1 La Bbox

Il arrive parfois que le constructeur d'un équipement implémente mal un protocole ou un algorithme de génération de clefs. C'est ce qui est arrivé à la Bbox, construite par Thomson.

Par défaut une Bbox émet un SSID<sup>1</sup> sous la forme : Bbox-xxxxxx. Les 6 derniers caractères xxxxxx sont ceux qui nous intéressent car l'algorithme de génération des clefs WPA par défaut des Bbox va se servir d'eux pour générer sa clef.

Vous avez bien compris, il suffisait d'observer le nom du réseau pour en déduire sa passphrase, moyennant l'utilisation d'un petit logiciel, Bbkeys, disponible sous Linux comme sous Windows : l'opération ne prend que quelques secondes et est d'une simplicité enfantine.

Ce type de vulnérabilité n'est pas nouveau, on a déjà pu l'observer sur les routeurs TECOM de l'opérateur Club Internet, ou sur les Speedtouch de Thomson. C'est bien le même algorithme cassé de Thomson qui est en cause.

Bouygues a déployé par la suite un nouveau firmware pour corriger cette faille.

### 3.2 Numéricable

Numéricable doit gérer le lourd passif de Noos en matière de mauvaises pratiques. Le câblo-opérateur fournissait à ses clients un modem/routeur Thomson

---

<sup>1</sup>Service Set Identifier - nom du réseau WiFi

doté du WiFi, activé par défaut, sans aucune protection, diffusant ainsi un réseau complètement ouvert exposant le trafic web de ses clients à toutes les écoutes et interceptions possibles, sans le moindre effort.

Pire, l'interface du routeur qu'il fournissait était uniquement disponible en anglais ! Il est déjà difficile pour beaucoup d'utilisateurs de configurer correctement ces matériels depuis une interface en français.

Tous les réseaux WiFi nommés « THOMSON » complètement ouverts que vous trouvez encore aujourd'hui en environnement urbain sont l'héritage de Noos fait à Numéricable : un cadeau empoisonné qui risque de conduire très rapidement Numéricable à rappeler tous ces boîtiers et à les échanger.

Encore aujourd'hui, les routeurs SAGEM de Numéricable proposent toujours du WEP par défaut. Un décret d'application d'Hadopi va-t-il les contraindre à un chiffrement plus sérieux ?

### 3.3 Freebox

La Freebox est un cas à part. Free est le seul fournisseur d'accès à observer de bonnes pratiques. Par défaut le WiFi n'est pas activé, il faut explicitement le mettre en route via la console d'administration pour pouvoir en profiter. Si on peut regretter d'avoir à passer par son site web pour configurer sa box, Free propose une information claire qui encourage ses abonnés à utiliser le WPA/CCMP.

Free rend également la tâche plus complète aux attaques informatiques : l'opérateur a mis en place une protection contre l'injection de paquets ARP, rendant bien plus longues les attaques sur les protocoles faillibles.

Autre point à noter, il est impossible sur une Freebox d'activer le WiFi et de le laisser sans aucune protection comme c'est le cas chez d'autres fournisseurs d'accès. Si vous souhaitez un réseau complètement ouvert, il vous faudra un matériel supplémentaire non fourni par Free.

Seule ombre au tableau : s'il vous est déjà arrivé de téléphoner à la hotline pour configurer le WiFi de votre box, vous avez peut-être entendu un technicien vous suggérer de choisir en mot de passe votre numéro de téléphone, celui-ci étant composé de 10 caractères hexadécimaux, il présente toutes les caractéristiques du parfait mot de passe. Une très mauvaise pratique : je vous laisse méditer sur le parfait dictionnaire d'attaque que représente un annuaire téléphonique.

Voici à quoi ressemble une configuration WiFi sécurisée sur une Freebox (notez que masquer un réseau n'est pas une réelle protection, si le réseau est invisible par le système de détection proposé en standard par votre système d'exploitation, n'importe quel scanner sera en mesure de le détecter, ne vous fiez donc jamais à ce seul artifice).

Le Freebox PCCV active automatiquement une liaison WiFi pour les clients Freebox PCCV, que le réseau WiFi personnel soit utilisé ou non. Cette option permet de désactiver complètement l'émission d'ondes WiFi par le Freebox.

Attention, si vous cochez cette case, les Freebox HD ne pourront être branchées que par câble ethernet ou par un Freeplug.

Activer le réseau wifi personnel:  Activer

Choisissez parmi la liste des canaux celui que vous souhaitez utiliser pour votre réseau WiFi. Si votre réseau WiFi souffre de lenteur ou de déconnexions fréquentes, tentez de changer le canal utilisé pour réduire les interférences.

Canal:

Si vous activez le choix automatique du canal, le Freebox choisira elle-même, à chaque démarrage, le canal WiFi le moins perturbé. Cela vous permet d'obtenir une connexion plus fiable.

Canal automatique:  Activer

Choisissez le nom de votre choix pour votre réseau WiFi.

Réseau:

Si vous le désirez, votre réseau WiFi peut être masqué, il devient donc invisible lors des recherches de réseau. Afin de faciliter la configuration de votre ordinateur, il est préférable de laisser cette option désactivée.

Réseau masqué:  Activer

La clé WEP ou WPA permet à votre ordinateur d'être authentifié auprès de votre Freebox et empêche que d'autres ordinateurs puissent utiliser votre liaison internet sans fil.

L'utilisation d'une clé WPA est préférée car elle offre une sécurité plus importante que la clé WEP. Vérifiez toutefois que votre système d'exploitation supporte le WPA si vous optez pour ce mode de protection.

Le mode WPA (TKIP+AES) est recommandé. Si vous rencontrez des problèmes pour connecter certains appareils (PDA/console de jeux...) essayez les modes WPA (TKIP) ou WPA (AES/CCMP).

Protection:

- WEP
- WPA (TKIP)
- WPA (AES/CCMP)
- WPA (TKIP + AES)

Entrez ci-dessous la clé WEP ou WPA que vous souhaitez utiliser. Une clé longue est plus sûre qu'une clé courte.

- Une clé WEP doit avoir une taille de 10 ou 26 caractères hexadécimaux (de 0 à 9 et de A à F)
- Une clé (ou "phrase de passe") WPA peut avoir une taille comprise entre 8 et 63 caractères. Le choix des caractères est libre.

Clé:

### 3.4 Combien Hadopi va t-elle coûter à l'opérateur ?

Manque d'information et inconscience des utilisateurs Peu de fournisseurs d'accès proposent une interfaces d'administration du WiFi claire et des informations claires sur les bonnes pratiques à adopter. Ajoutez à ceci une pratique commune qui consiste à choisir le nom du chat ou des enfants comme mot de passe pour s'authentifier au réseau, et la mine d'or d'informations que représente un Facebook ou un MySpace... Le nombre d'utilisateurs se croyant à l'abri mais qui utilisent un mot de passe trop simple est phénoménal.

## Chapitre 4

# Le WiFi dans les lieux publics

Il existe plusieurs types de réseaux publics :

- Le WiFi complètement ouvert dans les cafés, Hôtels ou restaurants : gageons que ces réseaux sont appelés à disparaître, à moins que les établissements n'investissent dans un système plus lourd proposant une authentification.
- Des réseaux nécessitant une authentification via un portail captif. Le concept est assez simple : vous vous connectez à un réseau qui semble non sécurisé, il n'est pas chiffré, et vous arrivez sur une page d'accueil où il vous est demandé de vous authentifier par le biais d'un radius (identifiant/mot de passe) sensé être suffisant pour vous identifier. Notez que ces réseaux sont généralement vulnérables à un contournement de cette identification mais ceci nécessite un bon niveau technique<sup>1</sup>. Il arrive aussi que ces points d'accès soient eux mêmes soit mal configurés (mot de passe du routeur inchangé permettant à n'importe qui d'en prendre le contrôle après avoir identifié<sup>2</sup> son constructeur grâce à l'adresse MAC émise par le point d'accès, son adresse ip avec une simple requête traceroute, et enfin son mot de passe par défaut sur l'un des sites<sup>3</sup> qui les recense).
- D'autres modes d'authentification sont bien évidemment envisageables, en Italie, il n'est par exemple pas rare de vous faire scanner votre carte d'identité pour pouvoir accéder à Internet en WiFi dans les hôtels. Dans les gares, vous disposez mêmes de machines destinées à laisser une « preuve » de votre identité pour accéder au Net... c'est effrayant, mais c'est bien ce qui nous pend au nez en France. Notez que cette procédure, coûteuse et très intrusive, permet à n'importe qui de faire scanner par la machine la carte d'identité d'un tiers.

Voici le genre de paramètres que vous trouvez en clair dans une URL de connexion à un point d'accès, l'exemple vient ici d'une connexion sur un point d'accès ADAEL. Ici la connexion ne nécessite pas d'authentification par mot de passe, l'accès est anonyme, mais vous pourriez observer qu'il collecte tout de même l'adresse MAC, (ici 00-18-39-C4-A2-BD), une adresse IP locale (192.168.100.25)

---

<sup>1</sup>Encapsulation TCPIP over DNS : <http://code.kryo.se/iodine/>

<sup>2</sup>Trouver le constructeur et le modèle d'un routeur grâce à son adresse MAC : [http://www.coffey.com/mac\\_find/](http://www.coffey.com/mac_find/)

<sup>3</sup>Trouver le mot de passe par défaut d'un routeur : <http://www.routerpasswords.com/index.asp>

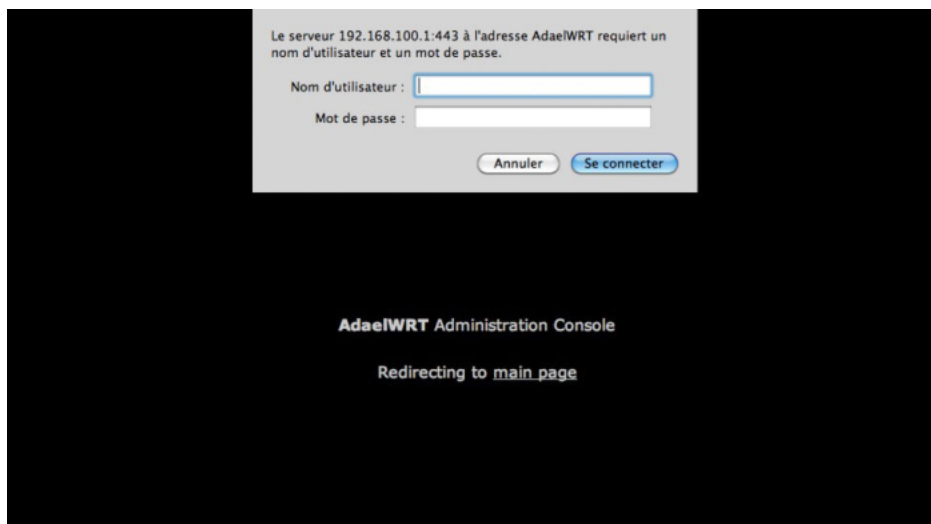
et un identifiant de session... bref, rien qui ne vous permet de vous identifier de manière formelle.

```
http://login.adael.com/bogorys/login?res=success&uamip=192.168.100.1&uamport=3990&uid=whqkafllssed@type1&timeleft=1200&mac=00-1E-52-73-62-6A&ip=192.168.100.25&called=00-18-39-C4-A2-BD&nasid=bogorys&redirurl=&userurl=http://conn.skype.com/&md=2B859C1B08141D7EED80886920BF23BE&c=1
```

On distingue très clairement l'adresse locale du point d'accès, ici : 192.168.100.1. De toutes façon, un simple traceroute permet de localiser ce même point d'accès.

```
Stolychnaya:~ bluetouff$ traceroute google.fr
traceroute: Warning: google.fr has multiple addresses; using 216.239.59.104
traceroute to google.fr (216.239.59.104), 64 hops max, 52 byte packets
 1 192.168.100.1 (192.168.100.1)  9.394 ms  3.773 ms  1.721 ms
```

Pour tester cette ip, il suffit de vous rendre avec votre navigateur sur cette adresse IP, vous y découvrirez l'accès à l'interface d'administration, dans notre exemple elle ressemble à ceci :



ADAEL propose donc un point d'accès dont le Firmware est basé sur Open-WRT ou DDWRT, deux firmwares libres basés sur GNU/Linux. Il n'est pas rare que des établissements proposant des connexions de ce type oublient de changer le mot de passe par défaut de leur point d'accès, même si je soupçonne ADAEL de faire du bon travail, les pratiques de certains clients peuvent conduire à de petites catastrophes, comme ce fut le cas à la gare du Nord<sup>4</sup> il y a quelques temps où un pirate a pris le contrôle d'un routeur.

<sup>4</sup><http://www.canardwifi.com/2007/06/07/surcharge-a-la-gare-du-nord/>

# Chapitre 5

## Démonstrations

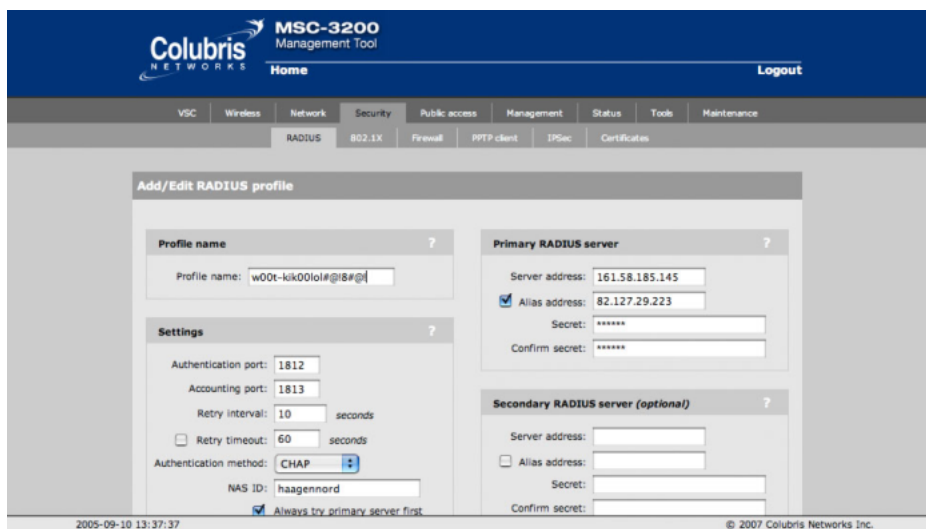
### 5.1 Routeur - réseaux payants

Ce routeur déployé par ADAEL<sup>1</sup> hébergeait tous les réseaux payants Orange/ Bouygues/Neuf/ADAEL... je les ai ouverts et j'en ai créé quelques autres)

```
Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2007-05-31 07:31 CEST
Initiating SYN Stealth Scan against access.adael.net (192.168.2.1) [1663 ports]
] at 07:31
Discovered open port 22/tcp on 192.168.2.1
Discovered open port 53/tcp on 192.168.2.1
Discovered open port 80/tcp on 192.168.2.1
Discovered open port 443/tcp on 192.168.2.1
Discovered open port 8082/tcp on 192.168.2.1
Discovered open port 448/tcp on 192.168.2.1
Discovered open port 8080/tcp on 192.168.2.1
Discovered open port 8081/tcp on 192.168.2.1
The SYN Stealth Scan took 4.26s to scan 1663 total ports.
For OSScan assuming port 22 is open, 1 is closed, and neither are firewalled
Host access.adael.net (192.168.2.1) appears to be up ... good.
Interesting ports on access.adael.net (192.168.2.1):
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
161/tcp   filtered snmp
443/tcp   open  https
448/tcp   open  ddm-ssl
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
8082/tcp  open  blackice-alerts
MAC Address: 00:03:52:03:EE:9E (Colubris Networks)
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.6 - 2.4.21
Uptime 14.617 days (since Wed May 16 16:42:52 2007)
TCP Sequence Prediction: Class=random positive increments
Difficulty=4200959 (Good luck!)
```

<sup>1</sup><http://www.adael.net/>

Sur le screenshot suivant, j'ai pris le contrôle du serveur radius pour l'authentification, j'aurai par ce biais pu récupérer les numéros de carte de crédit des personnes qui souhaitaient bénéficier d'une connexion sur des réseaux opérateurs<sup>2</sup>.



Les réseaux publics/privés sont de loin les plus intéressants et méritent qu'on s'y arrête, nous allons les subdiviser en deux catégories :

Les réseaux des opérateurs (type Neuf WiFi ou Free WiFi) : là où ce type de réseau, initié par Neuf, propose à l'internaute nomade de bénéficier de la NeufBox d'un autre Neufnaute (et donc de son adresse IP), Free a innové en proposant l'attribution d'une adresse IP publique spécifique au Freenaute qui se connecte sur la Freebox d'un autre Freenaute.

FreeWiFi est donc actuellement un réseau sur lequel les Freenautes partageurs ne risquent pas de se voir accusé de faits dont ils ne sont pas responsables. Les autres opérateurs devront s'aligner afin de proposer ce genre d'architecture s'ils ne veulent pas que leurs abonnés ne soient accusés à tort.

Là encore on attend les décrets d'application qui viendront définir le délit de négligence caractérisée mais ceci risque fort d'être croustillant quand les opérateurs concernés s'apercevront que ceci va avoir un coût. La question du financement des petits aménagements qu'implique Création et Internet reviendra très vite sur le tapis.

Les réseaux sociaux de types FON<sup>3</sup> ou les réseaux maillés de type OpenMesh<sup>4</sup> : ces réseaux sont eux aussi basés sur le partage, ils impliquent qu'un wifiste ait suffisamment confiance pour partager leur connexion.

<sup>2</sup>Le roman photo du hack est ici : <http://www.toonux.org/geekshots/geeks-hacking-wallpapers/wifi-gare-du-nord-0wn3d/>

<sup>3</sup>FON : <http://www.fon.com/fr/> : la plus grande communauté de wifistes partageurs au monde

<sup>4</sup>OpenMesh : <http://open-mesh.com>

Dans le cas de FON, par défaut, seulement les *foneros* peuvent accéder au réseau. Ils ont un identifiant et un mot de passe avec lequel ils établissent la session. Manque de chance, Hadopi ne sera pas en mesure de distinguer le trafic d'un *fonero* nomade de celui du propriétaire de la connexion, et c'est bien ce dernier qui recevra les mails d'avertissement en cas de téléchargement illégal. Le wifiste partageur devra donc contester ce mail et demander à FON de lui fournir l'adresse MAC (falsifiable aisément par un wifiste un peu malin), le compte du fonero (informations sur l'identité invérifiables de manière formelle) et la durée de session... c'est à dire pas grand chose mais c'est effectivement tout ce que FON pourra lui fournir car ce genre de système WiFi ne propose aucun mécanisme fiable d'authentification (pas plus que ne l'est une adresse IP, n'en déplaise au ministère de la Culture).

Le juge devra donc prendre sa décision à partir d'éléments non fiables, ne pouvant en aucun cas être considérés comme des preuves irréfutables.

Notez que FON risque surtout de souffrir d'une crise de confiance des utilisateurs qui préféreront éteindre leur Fonera plutôt que de courir un risque de se faire couper la connexion. FON pourrait être une victime d'Hadopi, ce qui est fort dommage vu que la communauté française<sup>5</sup>, l'une des plus importante au monde, est particulièrement dynamique.

Les réseaux maillés vont, eux, poser beaucoup de problèmes : ils peuvent être complètement ouverts ou chiffrés, vous avez le choix au déploiement, il ne permettent pas de donner d'autres informations que l'adresse MAC et la durée de session si on ne les couple pas à un portail captif et à un serveur radius (tous les protocoles de maillage ne les supportent pas).

Ils attribuent à l'internaute nomade l'adresse ip du modem (qui devient donc une passerelle) connecté à internet le plus proche. Si cette passerelle a une avarie, le réseau est assez intelligent pour lui attribuer l'adresse IP externe d'un autre passerelle présente sur le réseau, même si beaucoup plus éloignée.

Choses amusante, ils sont tout à fait capables de fonctionner sans connexion à l'Internet... en mode purement local donc sans risque de se faire attraper par Hadopi.

Ce genre de réseaux pourraient très vite proliférer en environnement urbain. Chiffrés ou totalement ouverts, ils pourraient devenir un fantastique outil de partage en réseau local. En standard Open-Mesh propose la fonctionnalité « join Network » qui permet à un utilisateur en possession d'un matériel compatible (une simple fonera reflashée ou le superbe et peu coûteux OM1P<sup>6</sup>) d'étendre un réseau existant en répétant le signal de ce dernier pour couvrir une zone plus vaste.

Les réseaux maillés sont à la fois un problème et une solution : ils pourront

---

<sup>5</sup>[www.francofon.fr](http://www.francofon.fr)

<sup>6</sup><https://www.open-mesh.com/store/categories.php?category=Professional-Mesh>

faire accuser à tort un wifiste partageur, inversement, ils pourront servir à contourner Hadopi de manière radicale et très efficace<sup>7</sup>.

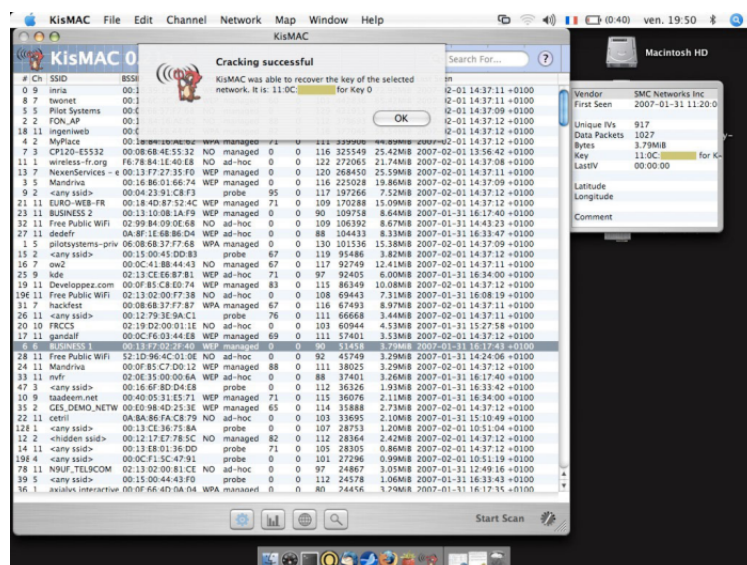
Une autre caractéristique fort intéressante en matière de sécurité et à porter au crédit d'Open-Mesh est le concept d'isolation des utilisateurs. Ainsi, sur l'accès ouvert et public, il n'est pas possible pour un utilisateur de scanner le trafic et d'intercepter les données d'autres utilisateurs. La connexion est bridée, il ne sont pas sur la même plage ip, ils ne peuvent même pas se pinguer mutuellement. Cette fonctionnalité particulièrement intéressante devrait être généralisée sur tous les réseaux ouverts, elle évite les interceptions directes sur le réseau par sniffing de paquets (avec wireshark, tcpdump ou la suite dsniff).

## 5.2 Les pratiques des entreprises

En entreprise, le WiFi est également largement adopté, cependant les bonnes pratiques en matière de sécurité sont régulièrement passées à la trappe. Mais il existe des endroits où les entreprises s'exposent encore plus que dans leur propres locaux : lorsqu'elles sont en déplacement dans des salons professionnels.

Les salons sont un véritable paradis pour les pirates, ils peuvent avec très peu d'efforts accéder à des données d'entreprises peu soucieuses de la sécurité de leur connexion. Une fois sur le réseau, c'est la porte ouverte à toutes les interceptions, mots de passe, emails...

Voici des captures d'écran prises en 2007 sur un salon professionnel au CNIT de la Défense à l'occasion du salon Solution Linux, regroupant pourtant des professionnels sensés savoir ce qu'ils font, le WPA n'était franchement pas la norme.



<sup>7</sup><http://bluetouff.com/2009/04/27/contourner-Hadopi-echange-local-wifi-maille/>

## Chapitre 6

# Conclusion

Si vous n'êtes pas en possession d'une Freebox V5 et de matériel compatible, vérifiez vos paramètres si vous ne voulez pas avoir la mauvaise surprise de recevoir des courriers d'avertissement de la Haute Autorité, et d'avoir à expliquer à cette dernière que par défaut, votre opérateur ne vous fournit ni les moyens techniques, ni l'information nécessaire pour protéger votre réseau WiFi.

La Hadopi vient poser les bases d'une justice qui va devoir s'arracher les cheveux pour déterminer les responsabilités des uns et des autres. La sécurité est un processus et non un produit, c'est malheureusement donc sa définition même qu'Hadopi a souhaité occulter en érigeant l'utilisateur abonné au rang d'expert de la sécurité.

Pour le tranquilliser, le législateur a même poussé le bouchon jusqu'à lui proposer un « logiciel de sécurisation », non interopérable, payant, et qui dans les faits ne sécurisera rien du tout.

Bien au contraire, il y a fort à parier que ce logiciel créera de l'insécurité. L'utilisateur pensera que ce logiciel agit comme un pare-feu (la définition du firewall de Christine Albanel avec OpenOffice nous laisse augurer du pire). Cependant, ce logiciel, qu'il convient de considérer comme un simple mouchard, ne sécurisera ni votre connexion, ni votre système d'exploitation, venant ajouter un peu plus de confusion sur ces problématiques déjà complexes.

Enfin, les opérateurs y trouveront sûrement leur compte pour vous vendre une soit disant sécurité absolue en option à 5 euros par mois, en partenariat avec tel ou tel éditeur antivirus.

Si vous n'êtes pas un virtuose de la base de registre de Windows un administrateur système curieux et aux compétences à jour ou bien un expert en chiffrement, vous êtes tous potentiellement menacés de vous rendre coupable de négligence caractérisée.

Nous avons vu que le WiFi pourrait poser de nombreux problèmes et apporter de nombreuses solutions. Prendre le risque de mettre en péril cette technologie largement adoptée dans les usages de millions d'internaute est loin d'être

une solution viable, surtout à l'heure où ce type de technologie sans fil pourrait servir à réduire la fracture numérique en acheminant du débit dans des zones qui ne sont toujours pas desservies en ADSL.

Autre risque important, faire du WiFi, technologie déployable et accessible par tous, une technologie opérateurs payante car ils deviendront les seuls en mesure d'attribuer des adresses IP publiques et de fournir un niveau d'authentification des utilisateurs acceptables. La mort des petits opérateurs WiFi est donc annoncée.

On ne peut que déplorer que le législateur ait fait l'impasse sur cette somme de détails qui font de 90% des internautes français, particuliers, comme entreprises, des présumés coupables.