Septembre 2003

MOUCHARDS INFORMATIQUES

De l'atteinte à la vie privée à l'espionnage des états

Principes, Techniques et Législation

Laure Brignone

DESS Audit et Expertise en Informatique
Université Paris II Panthéon-Assas

Mémoire préparé sous la direction de Monsieur Jean Donio

Remerciements

Monsieur Jean DONIO	Directeur du DESS audit et expertise en informatique et techniques numériques.
Monsieur Frédéric PRETO	Consultant Indépendant
Monsieur Ely DETRAVIESO	Chef de Projet - Detectiva-Interactive
Mademoiselle Déborah DJIAN	Ingénieur Système - LogicaCMG
Monsieur Marc BLANCHARD	Directeur du Centre de Recherche Antivirus - Trend Micro
Monsieur Jean BURNOD	Fondateur - E-Picture Certification.
Monsieur Fabrice LALANDE	Directeur technique - E-Picture Certification.

Ainsi qu'à toutes les personnes ayant mis en libre accès leurs recherches, études, mémoires sur les différents sujets abordés.

Egalemet à toutes les personnes qui ont contribué de plus ou moins loin à la rédaction de ce mémoire par leurs avis, idées et corrections.

Table des matières

Avant propos 06
- Terminologie..... 07
- Classification..... 08
- Quelques principes juridiques sur les données personnelles et le respect de la vie privée..... 10

1er chapitre : Les Mouchards Dédiés 12

I / Les mouchards logiciels ou spyware 13

1.1 / Les moyens de propagation 13
1.2 / Quelques types de mouchards logiciels 14
1.2.1. Le spyware de RealJukebox
1.2.2. Le spyware d'ICQ
1.2.3. Alexa ou Related Info
1.2.4. BHO (Browser Helper Objects)
1.3 / L'utilisation de ces informations ou les dispositifs marketing de la net économie 15
1.4 / Les justifications de leurs usages et le modèle économique du net 16
1.5 / La législation française et européenne 17
1.6 / Les licences d'utilisation 18
1.7 / La détection et les contre-mesures 20
1.7.1. Prévention
1.7.2. La détection et l'éradication
1.7.3. Le P3P : Platform for Privacy Preferences Projet

II / Les codes malicieux utilisés comme mouchard : Les Chevaux de Troie 22

2.1 / Principe 22
2.2 / Classification 23
2.2.1. Les chevaux de Troie d'administration à distance (RAT)
2.2.2. Les chevaux de Troie FTP
2.2.3. Les chevaux de Troie de mots de passe
2.2.4. Les enregistreurs de touches ou key loggers
2.3 / Les différentes utilisations des chevaux de Troie 25
2.4/ Détection et éradication 26

III / Les réseaux d'espionnage d'États ou les systèmes de surveillance et d'interception électronique 27

3.1 / Le système Échelon 27
3.1.1. Principe de fonctionnement
3.1.2. Les doutes sur l'espionnage économique
3.1.3. Le problème des libertés individuelles : les atteintes à la vie privée
3.1.4. Les limites du système Échelon
3.2 / Carnivore ou DCS1000 30
3.2.1. Historique du projet et validité vis à vis de la loi
3.2.2. Principe
3.3 / Les autres projets d'États 31
3.3.1. Suisse : Satos-3
3.3.2. France : surnommé Frenchelon par les anglo-saxons
3.3.3. Russie : Sorm-2 (System of Efficient Research Mesures)
3.3.4. Les autres pays
3.4/ La législation française sur le sujet 32

2ème chapitre :
Utilisations détournées, abusives de ressources normales 33

I / Les Guid (Global Unique Identifier) 34

II / Les cookies et Web bugs 37
2.1 / Les cookies (ou témoins de connexion) 37
2.1.1. Fonctionnement
2.1.2. Utilisation
2.1.3. Les moyens de prévention contre une utilisation abusive
2.2 / Les Web bugs ou 1-pixel gifs (pixels invisibles) 39
2.3 / La législation 40

III / Les fichiers logs 42
3.1 / La législation française sur les fichiers logs 42
3.2 / Les « recommandations » du G8 sur les logs de connexion 43

IV / Les autres ressources à risque 45
4.1 / Les VBScripts, la technologie Active X et les CGI 45
4.1.1. Les scripts CGI (Common Gateway Interface)
4.1.2. Les VBScripts
4.1.3. La technologie Active X

4.2 / Les failles de logiciels et systèmes d'exploitation 46
4.3 / Les réseaux sans fil 47

V / Les contre-mesures 49
5.1 / Les firewalls (pare feu) : protecteur ou espion ? 49
5.2 / Les proxies et techniques d'anonymat 49
5.3 /Les projets sécuritaires : TCG et Palladium 50
5.3.1. Le Trust Computing Group et TCPA
5.3.2. Le NGSCB ou Palladium
5.3.3. Les buts de ces projets
5.3.4. Les risques économiques
5.3.5. La possibilité de désactivation
5.3.6.Au niveau du droit

Conclusion 56

Annexes 58
Annexe 1 : Les articles du Code Pénal relatifs à la vie privée. 58
Annexe 2 : Résumé de la législation européenne sur la vie privée. 59
Annexe 3 : La liste des logs de connexion dressés par Europol. 61

Bibliographie 64

Avant propos

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »
(Article 1er loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Le respect de la vie privée : la liberté individuelle. C'est la protection de l'environnement de l'individu sur le plan de l'information, c'est-à-dire le droit de l'individu à contrôler ou agir sur des informations qui peuvent être collectées ou stockées.

Ce dossier est très vaste car il touche à plusieurs sujets liés au monde de l'informatique, à de nombreux points juridiques mais aussi économiques.

La problématique du mouchard informatique ne s'arrête pas aux spywares logiciels, elle inclut également des projets et des technologies. En effet, le vrai problème est que toute technologie liée à l'informatique peut être détournée et devenir un mouchard. De plus, il se situe à deux niveaux : l'intrusion dans les réseaux informatiques (informations stockées) mais aussi l'intrusion sur les réseaux de communication (informations en transit).

Ce sujet soulève plusieurs problématiques :

- Les problèmes liés à la sécurité, tant au niveau des systèmes d'information que plus globalement ainsi que la confidentialité et l'anonymat.

En effet, l'anonymat et la cryptographie peuvent être une parade à ces mouchards. Pourtant la cryptographie ne sera pas abordée dans ce dossier car il s'agit d'un sujet à part entière, nous y ferons donc simplement référence pour certaines contre-mesures.

Le mouchard est une menace à la confidentialité des informations. Il peut éventuellement toucher la disponibilité lorsqu'il provoque un ralentissement trop important mais cela n'est en général pas visible puisqu'il se veut furtif. Certains peuvent également être une menace à l'intégrité de l'information, en particulier dans le cas des chevaux de Troie.

- Le modèle économique du net est un grand débat, sa gratuité étant utilisée comme justification aux spywares logiciels mais également des risques d'espionnage économique voire politique.

- La question de la vie privée qui découle du problème de confidentialité : il est difficile de fixer une limite juridique car beaucoup d'éléments entrent en ligne de compte. Ainsi les lois contre la fraude et les techniques mises en œuvre pour assurer une meilleure sécurité vont souvent à l'encontre de la vie privée.

De plus il est difficile de déterminer un périmètre d'analyse des mouchards informatiques, toutes les technologies pouvant être détournées. Il y a donc un problème de terminologie et de périmètre qu'on se propose d'expliciter.

Terminologie

Espiogiciel ou espiologiciel (spyware en anglais) :

Le terme anglais vise toute technologie qui permet de récupérer des informations sur une personne ou une société sans qu'il en soit informé.

En informatique, c'est un module logiciel et par extension un programme permettant de collecter de manière sélective des informations sur ses utilisateurs (configuration matérielle et/ ou logicielle, habitudes d'utilisation, données personnelles…) puis de les transmettre à son concepteur ou à un tiers (régies publicitaires…) via Internet ou tout autre réseau informatique, sans avoir au préalable obtenu une autorisation explicite et éclairée de l'utilisateur, peu importe qu'il y ait ou non un rapprochement entre ces informations et l'identification du dit utilisateur.

Ils se trouvent généralement dans le code d'un programme que l'utilisateur télécharge innocemment sur internet. Dans la plupart des cas se sont des « petits morceaux de code parasites » (routines) intégrés dans le code principal du programme. Ce n'est pas un virus.

Ce terme se réfère surtout, et encore plus dans sa traduction française, aux logiciels servant à regrouper des informations à des fins commerciales. Le terme anglais de spyware peut être utilisé dans un sens plus large, mais l'on préférera ici le terme de mouchard informatique, terme à connotation plus vaste. Cependant il faudra en préciser les limites dans le cadre de ce mémoire, bien que dans le vocabulaire informatique, le terme de mouchard et plus particulièrement de mouchard électronique est surtout utilisé pour définir les cookies.

De façon plus générale, mouchard signifie : indicateur, espion ou nom de certains appareils de contrôle et de surveillance (hachette). Un mouchard dans le sens où nous l'entendons dans ce mémoire est une fonction cachée, résidente, matérielle et/ou logicielle.

Classification

La classification des mouchards informatiques est difficile, puisque toute technique ou technologie informatique peut être détournée à des fins d'espionnage. Si on se situe au niveau des espiogiciels, on peut alors avoir une classification car ils sont répertoriés (pour ceux qui sont connus) dans de nombreuses listes (remises à jour régulièrement).
En revanche, il devient très difficile de définir toutes les techniques pouvant intervenir, d'une part parce que cela couvre l'informatique dans son ensemble et d'autre part, ce domaine évoluant très vite, de nouvelles techniques et des utilisations détournées apparaissent en permanence, ainsi que de nouveaux projets. On a donc répertorié les plus importantes ou en tout cas les plus visibles, mais cette liste est loin d'être exhaustive.

- Un premier classement pourrait être fait en distinguant ce qui est logiciel (dont le système d'exploitation) du matériel mais il n'est pas pertinent, puisqu'un mouchard matériel est souvent associé à un logiciel, et que ce classement n'inclut pas de distinction entre les solutions dédiées et non dédiées.

- Classement en fonction de leurs buts et donc des différents acteurs, utilisateurs de ces mouchards :

  - les régies publicitaires, éditeurs de logiciels et certains fournisseurs d'accès : ils cherchent à établir des profiles d'internautes et à créer d'immenses bases de données regroupant le plus d'informations possible, à des fins commerciales, de marketing et de statistiques. Ils utilisent des spywares logiciels mais aussi les cookies, les web bugs, les guid…

  - Les services de renseignement des grands pays industrialisés : à des fins de sécurité ou d'espionnage industriel. Ils utilisent en général toutes les technologies pouvant être détournées de leur utilisation d'origine de manière à pouvoir recouper les informations et retrouver les sources.

  - Les hackers, par pure prouesse technique. Ce sont en général eux qui trouvent en premiers les différentes failles et les outils qui peuvent être détournés de leur utilisation originelle. Ce sont également eux qui créent les codes malicieux comme dans notre cas les chevaux de Troie par exemple.

  - Les entreprises peuvent utiliser des mouchards ou des outils permettant de tracer l'activité du salarié. Mais cela doit être fait en respectant une législation bien précise et ne doit pas se confondre avec les mesures de sécurité du système informatique de l'entreprise.

  Mais ces différents acteurs utilisent des technologies communes.

- Classement par types de vulnérabilités des systèmes d'information et de communication, moyens permettant de récupérer des informations :

  - l'écoute passive : écoute de signaux par interception des liaisons satellitaires ou des faisceaux hertziens, par branchement sur les réseaux filaires ou écoute des réseaux. Ce

sont les systèmes d'interception électroniques. C'est l'intrusion sur les réseaux de télécommunication.

- L'écoute active : l'information est fournie par la source en raison de virus informatiques ou de chevaux de Troie introduits dans le système de l'émetteur. Les spywares rentrent aussi dans cette classification. C'est une partie des techniques d'intrusion dans les réseaux informatiques.

- Les intrusions : recherche de l'information au cours des interceptions GSM, attaques lors de télémaintenances, vols de session, usage de portes dérobées (backdoor) dans les systèmes d'exploitation… Nous parlerons très peu de ce point car le sujet porte ici sur les systèmes logiciels ou matériels d'espionnage, les techniques d'intrusions ne seront donc pas abordées.

- Finalement il nous a paru judicieux d'utiliser une première classification de mouchards dédiés et non dédiés.

Pour subdiviser les mouchards dédiés, nous utiliserons la classification en fonction des buts des acteurs :

- les espiogiciels ou spywares : recherche d'information dans un but commercial,
- les chevaux de Troie : espionnage, pirates informatiques…,
- les programmes d'État : Echelon, Carnivore et autres.

Nous aborderons ensuite toutes les technologies qui peuvent être détournées à des fins de profilage ou d'espionnage : Guid, Cookies et web bugs, fichiers log… mais aussi deux projets à la limite entre sécurité et vie privée, anciennement nommés TCPA et Palladium.

Les justifications de l'utilisation de ces mouchards sont selon leurs types, d'ordre économique ou sécuritaire. Nous verrons pour chacun leurs utilisations et justifications et les atteintes à la vie privée qu'ils peuvent engendrer en fonction des lois en vigueur tant au niveau français qu'européen. Nous aborderons très succinctement les lois américaines dans des points très précis.

Quelques principes juridiques de base sur les données personnelles et le respect de la vie privée

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »
Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, article 8

« Chacun a droit au respect de sa vie privée.
Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée ; ces mesures peuvent, s'il y a urgence, être ordonnées en référé. »
Code Civil : Article 9 (loi n°70-643 du 17 juillet 1970)

- Le traitement des données nominatives dépend de la CNIL (Commission Nationale de l'Informatique et des Libertés), qui est un organe indépendant veillant à l'application de la loi du 06/01/1978. Elle enregistre les plaintes, les instruit et peut prendre des sanctions, en général assez symboliques, mais elle peut aussi dénoncer l'affaire au parquet.

« Une Commission Nationale de l'informatique et des libertés est instituée. Elle est chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concertant avec elles et contrôlant les applications de l'informatique aux traitements des informations nominatives. La commission dispose à cet effet d'un pouvoir réglementaire, dans les cas prévus par la présente loi. »
(Chapitre 2 de la loi informatique et libertés du 6 janvier 1978)

- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés n'interdit pas la création de fichiers nominatifs, mais pour exploiter des données nominatives en tant que personne morale, il faut accomplir une formalité préalable auprès de la CNIL : tout traitement de données personnelles doit être déclaré à la CNIL. Pour le secteur privé une déclaration suffit, la CNIL n'a aucun pouvoir de blocage. Par contre le secteur public doit demander préalablement un avis à la CNIL et si l'avis est défavorable il ne peut passer outre sauf par décret gouvernemental.

Cette loi définit les informations nominatives :
« Sont réputés nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale. »
(Article 4)

Les données nominatives comprennent donc le nom, prénom, adresse, date de naissance, caractéristiques physiques, état civil… mais également une catégorie d'informations qui sont indirectement nominatives c'est à dire qui ne se réfèrent pas directement à la personne mais qui sont liées à elle (adresse IP, les Guid…).

On retrouve une définition proche dans la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, du 24 octobre 1995 :
« "données à caractère personnel", toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. »
(article 2)

Mais c'est dans la directive 2002/58/CE relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques, du 12 juillet 2002, qu'est précisé le comportement qu'il faut avoir vis à vis des mouchards informatiques :

« (24) L'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Or, les logiciels espions, les pixels invisibles (web bugs), les identificateurs cachés et les autres dispositifs analogues peuvent pénétrer dans le terminal de l'utilisateur à son insu afin de pouvoir accéder à des informations, stocker des informations cachées ou suivre les activités de l'utilisateur, et peuvent porter gravement atteinte à la vie privée de ce dernier. L'utilisation de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur concerné. »

Une présentation un peu plus précise des directives se trouve dans l'annexe 2 et l'on étudiera plus en détail la loi informatique et liberté lors de la première partie sur les espiogiciels.

Les mouchards dédiés

1er chapitre

Les mouchards dédiés regroupent principalement :

- Les logiciels appelés spywares ou espiogiciels qui ont comme but la collecte d'informations de manière à créer un profil commercial de l'internaute.

- Les codes malicieux ayant un rôle de mouchard : les chevaux de Troie et dérivés. Encore appelés backdoor pour certains, car ils utilisent une porte dérobée.

  Nous n'employons pas le terme de virus car les chevaux de Troie ne sont pas à proprement parler des virus. Le terme de code malicieux pourrait être utilisé car il est plus vaste et inclut les virus hybrides, chevaux de Troie et vers.

- Enfin les projets qui avaient ouvertement comme but la collecte d'informations en raison de sûreté nationale, projets de gouvernement comme Echelon et Carnivore : ce sont les réseaux d'espionnage d'États ou les systèmes de surveillance et d'interception électronique.

I / Les mouchards logiciels ou spyware

Un tiers des entreprises ont vu leur réseau informatique infecté par des logiciels spyware selon l'étude « Menaces Internet Émergences 2003 ». Les utilisateurs sont en effet très peu sensibilisés à ce problème.

Toutes les formes d'implants malveillants relèvent de la programmation qui peut prendre différentes formes :

- Programmes externes ou externalisés : codage distinct dans un programme autonome ayant son activité propre ou étant activé par l'hôte.

- Programmes internes ou intégrés : codage de l'espion intimement mêlé au code du programme hôte. Le spyware est alors une simple routine. Le spyware et le programme associé ne font qu'un et s'installent simultanément sur l'ordinateur de l'utilisateur.

Les principales informations envoyées sont :

- Les URL (adresses) des pages visitées permettant de déduire les centres d'intérêts marchands et le profil personnel de la personne.
- Tous les cookies
- Les informations sur le navigateur et l'historique
- L'adresse IP de l'ordinateur
- Les GUID des différents matériels et logiciels et donc le système d'exploitation, les caractéristiques techniques de tout le matériel contenant le pc et les différents logiciels installés.
- ….

1.1 / Les moyens de propagation

- Par la navigation sur Internet : par la technologie active X, certains programmes s'installent directement lorsqu'on arrive sur une page Internet, sur les sites contenant des web bugs…

- Par le téléchargement de adware (logiciels contenants de la publicité) ou de freeware (logiciels gratuits).

  - Un adware est un programme pouvant paraître gratuit mais qui est en fait supporté par la publicité ou des services tiers. Un bandeau publicitaire est rafraîchi périodiquement via Internet. Certaines régies publicitaires ont voulu cibler ces publicités, le adware dans ce cas contient alors un spyware.

- De plus certains logiciels gratuits intègrent dans leur interface, un ou plusieurs spywares qui sont soit internes soit qui se chargent en même temps que le logiciel.

En effet de nombreux logiciels (freeware ou adware) ont plus ou moins des mouchards intégrés :
- En particulier les messageries instantanées qui sont très dangereuses au niveau de la sécurité (mouchard d'ICQ).
- Dans les lecteurs audio : Realjukebox de Realnetworks.
- Les systèmes peer to peer (poste à poste ou de point à point) : le plus connu à contenir de nombreux mouchards est Kazaa mais il en existe plusieurs autres dont Limewire et Morpheus.

- Par le système d'exploitation et les applications commerciales correspondantes : procédure d'enregistrement en ligne, commerce en ligne…

On retrouve ces différents points dans l'étude « Menaces Internet Émergentes 2003 » puisque les trois grandes préoccupations des professionnels de l'informatique sont la navigation personnelle (31%), le téléchargement de logiciels (24%) et les e-mails Web (24%). Le peer to peer représente 5% et les messageries instantanées 3%, en revanche 70% des professionnels pensent que le peer to peer créé une porte ouverte aux hackers.

1.2 / Quelques types de mouchards logiciels

1.2.1. Le spyware de RealJukebox

Ce logiciel est un lecteur de fichiers audio (lecture de cd audio, lecture de MP3 et encodage) de la société RealNetworks (éditeur de Realplayer).
Lors de l'enregistrement du programme, un Guid, identifiant unique contenant l'adresse Mac, était envoyé. Ce même Guid était envoyé lorsque l'on écoutait un cd audio ou un MP3 avec des informations sur les catégories des titres lus, le nombre de titres stockés sur le disque dur, les formats de fichiers… RealNetworks pouvait ensuite créer des fichiers sur les habitudes de téléchargement, les modes de consommation, les centres d'intérêt.
Après un procès, RealNetworks a été contraint d'éditer un correctif empêchant l'envoi des données et désactivant le Guid de RealJukebox.

1.2.2. Le spyware de ICQ

ICQ, logiciel de messagerie instantanée, intègre un mouchard qui fait l'inventaire des programmes et numéros de séries associés et qui le renvoie au serveur d'ICQ. Il est très facile à désactiver en allant dans la base de registre, il suffit d'être au courant...

1.2.3. Alexa ou Related info

Les Related Info sont des types de spywares : liens "intelligents" construits à la volée, généralement dans une barre de recherche comme le "volet d'exploration" du navigateur,

cherchant à envoyer l'utilisateur vers des sites choisis dans son intérêt ou dans l'intérêt financier du spyware… Les ventes qui en découlent rémunèrent au forfait ou au pourcentage l'éditeur de l'utilitaire.

Le plus connu est Alexa qui se greffe sur Internet Explorer. C'est un mouchard d'Amazon contenu dans zBubbles, compagnon logiciel pour Internet Explorer.
Le terme « related info » est utilisé soit de manière générale, soit pour définir ce type de liens intelligents greffés à Netscape.

1.2.4. BHO (Browser Helper Objects)

Ils apportent des caractéristiques ou des fonctionnalités, additionnelles ou de personnalisation, à un navigateur. Ils se présentent lorsqu'ils sont visibles comme une série de boutons ou une barre de boutons ajoutés au menu du navigateur. Ils modifient également la base de registre.
Ils ne fonctionnent qu'avec Internet Explorer ou ses clones.
Ils ont accès à tous les fichiers et actions effectuées par le navigateur : Ils peuvent ainsi intervenir sur le contenu de l'affichage, ont accès à toutes les informations envoyées à un site Web dont les mots de passe, les noms et toute autre information personnelle, et à tous les sites que l'on visite. Ils peuvent également envoyer des informations à un serveur.

Il y a plusieurs types de problème avec les BHO :
- Souvent mal écrits, ils provoquent des erreurs dans Internet Explorer et lorsque plusieurs sont installés, ils peuvent entrer en conflit.
- Nombre de BHO se comportent en spyware. Ils envoient alors les habitudes de navigation à un site marketing.
- Des codes malicieux peuvent s'ajouter au BHO et envoyer tous les mots de passe, des informations personnelles…

1.3/ L'utilisation de ces informations ou les dispositifs marketing de la net économie

- Les spywares permettent, grâce aux informations collectées, d'envoyer à chaque utilisateur de la publicité ciblée :

- Par des bandeaux publicitaires (bannières), en fonction de son profil, qui apparaissent sur certains sites.
- Par des pages pop-up qui apparaissent lorsque l'on ouvre l'explorateur ou lorsque l'on arrive sur certains sites toujours personnalisés.

C'est un des moyens du spam car beaucoup de spywares transmettent les adresses e-mails et peuvent ensuite envoyer des mails ciblés (ou non).

Ils peuvent même aller jusqu'à envoyer des publicités papier ou effectuer du marketing téléphonique.

- Ils peuvent suggérer des sites grâce au related info et donc envoyer l'internaute vers un site qui a été choisi pour lui et non par lui.

- Ces mouchards permettent surtout le traçage puis le profilage des internautes afin de constituer de gigantesques bases de données qui se vendent à prix d'or, en particulier pour les fichiers opt-in (c'est à dire lorsque la personne a donné son autorisation explicite : case à cocher).

1.4/ Les justifications de leurs usages et le modèle économique du net

Les régies publicitaires et sociétés de marketing donnent plusieurs justifications à leur usage :

- Les informations sont anonymes car elles sont traitées de manière agrégée.

C'est effectivement le cas pour tout ce qui est statistique mais sûrement pas pour les bases de données qui sont créées.

- Les informations sont insignifiantes.

On a vu que les informations récoltées sont des informations à caractère personnel d'après la loi informatique et liberté et la directive de 1995. Elles ne sont donc pas insignifiantes.

- Dans le but de mieux personnaliser les services et offres publicitaires qui seront proposés ensuite : publicité ciblée.

Cette justification est effectivement valable puisque dans de nombreux cas c'est le but de ces logiciels mais le problème est que ce n'est pas l'unique usage qui en est fait.

- Le modèle économique du net : les entreprises proposant des freewares (logiciels gratuits) doivent dégager un profit ailleurs et les spywares permettraient à ces entreprises de se rémunérer.

Pourtant le logiciel gratuit est déjà un moyen de faire connaître l'entreprise, et la plupart proposent ensuite, des versions payantes avec des fonctionnalités supplémentaires. Le logiciel gratuit est en lui-même une publicité pour l'entreprise, il permet de faire connaître ses produits.

De plus de nombreux logiciels gratuits ont des bannières publicitaires pour se rémunérer qui ne sont pas très gênantes quand elles sont placées dans un angle de l'écran. Elles sont donc rémunérées également par les régies publicitaires.

Les avis sur ce point sont très partagés. Certains disent qu'interdire les spywares serait la fin du logiciel gratuit. Il existe pourtant des logiciels gratuits ne contenant pas d'espiogiciel, et ils ne disparaissent pas pour autant.
Cette justification ne semble pas fondée, de plus pour les raisons que l'on a vu plus haut, l'entreprise dégage un bénéfice à proposer des logiciels gratuits.

En revanche, le spyware est effectivement un moyen efficace de sonder le futur client et d'effectuer à très grande échelle des enquêtes de consommation au niveau d'Internet, mais surtout de cibler l'éventuel acheteur qui pourrait être intéressé par tel ou tel produit.
Ce serait davantage un outil marketing entraînant un profit supplémentaire (ce qui est le but de tout outil marketing à plus ou moins long terme) et non pas l'unique rémunération.

Dire que ce profit supplémentaire est indispensable à l'existence du logiciel gratuit n'est pas justifié, car le logiciel gratuit peut être un outil marketing à lui seul. Le spyware n'est pas une obligation à l'existence de ce type de logiciel.

Les utilisateurs sont peu sensibilisés aux spywares et parmi ceux qui le sont, beaucoup considèrent que c'est le prix à payer pour le logiciel gratuit et que les informations divulguées ne sont pas importantes, étant donné que ces logiciels peuvent faciliter leurs recherches sur Internet.

1.5/ La législation française et européenne

A l'origine, toutes ces sociétés ne respectaient pas les lois sur la vie privée car l'internaute n'était pas prévenu avant la collecte d'informations (et même après). De nombreuses plaintes ont été déposées et il existe aujourd'hui une jurisprudence assez importante sur le sujet.

Pourtant le droit à l'information préalable était clairement précisé dans la loi informatique et libertés du 6 janvier 1978 :

Droit à l'information préalable :
Obligation d'information au moment de la collecte des données.
Les fichiers ne doivent pas être créés à notre insu : « *la collecte des données opérée par tout moyen frauduleux, déloyal ou illicite est interdite »* (art 25 chapitre IV)
Les personnes qui créent des traitements ne doivent pas laisser les internautes dans l'ignorance de l'utilisation qu'ils vont faire de ces données. Autrement la loi informatique et liberté est violée.

> *« Les personnes auprès desquelles sont recueillies des informations nominatives doivent être informées : du caractère obligatoire ou facultatif des réponses, des conséquences à leur égard d'un défaut de réponse, des personnes physiques ou morales destinataires des informations, de l'existence d'un droit d'accès et de rectification. »*
> (Article 27 de la loi, décret n°81-1142)

C'est pour cette raison que de nombreux procès ont eu lieu contre les spywares logiciels car précédemment les usagers n'en étaient pas du tout avertis (une mention est aujourd'hui indiquée bien que souvent elle ne soit pas très lisible ou compréhensible…) et l'installation d'un logiciel renvoyant des données privées est une atteinte à la vie privée au sens de cette loi.

> *« Il est interdit de mettre ou de conserver en mémoire informatique, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les*

origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes »
(article 31)

Il semble donc que toutes les techniques de profilage sont illégales car dans de nombreux cas elles peuvent définir des opinions politiques, mœurs…

Le droit d'opposition :
« Toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement. »
(Article 26 chapitre IV)

La loi garantit un droit d'opposition qu'on peut exercer au moment de la collecte ou plus tard, en demandant par exemple la radiation des données contenues dans les fichiers commerciaux. Ce droit ne s'applique qu'aux fichiers qui n'ont pas été rendus obligatoires par une loi.

Différentes formes d'expression de ce droit d'opposition :
- le refus de répondre lors de la collecte non obligatoire de données,
- la possibilité de demander la radiation des données contenues dans les fichiers commerciaux ou de vente par correspondance,
- la possibilité d'exiger la non-cession ou la non-commercialisation des informations.

La directive 2002/58/CE est encore plus précise sur le sujet (article 24), elle considère que ces logiciels (et autres) peuvent *« porter gravement atteinte à la vie privée »* et précise à nouveau que l'utilisation des spywares doit être «*portée à la connaissance de l'utilisateur concerné*».

Ces droits se retrouvent dans la plupart des législations sur la protection des données personnelles en Europe et dans le monde.

Le non-respect de ces lois entraînent des peines allant d'un an à trois ans d'emprisonnement et d'une amende.
(Voir pour plus de détail les articles du code pénal s'y référant dans l'annexe 1.)

1.6/ Les licences d'utilisation

Grâce aux lois sur la vie privée, après de nombreux procès, les éditeurs ont été obligés de préciser l'existence de ces spywares lors du téléchargement de logiciels gratuits en contenant. Le seul problème est que la clause contractuelle est en général indiquée en tout petit au milieu de dix pages de commentaires suivis de la clause de vie privée en général en anglais et rédigée de la même manière. Ils sont aussi présentés comme des fonctionnalités indispensables à prendre, nous facilitant la vie dans une case pré-cochée (opt-out).

- Opt-in : une personne donne son autorisation explicite à une entreprise pour utiliser ses informations personnelles dans un but marketing. En général il s'agit d'une case à cocher.

– Opt-out : une personne doit préciser à une entreprise de ne pas utiliser ses informations personnelles dans un but marketing. En général c'est une case pré-cochée qu'il faut donc décocher si on ne désire pas que nos informations personnelles soient utilisées.

Ainsi les utilisateurs, qui sont le souvent très jeunes,

- ne vont pas prendre le temps de lire les licences d'utilisation en général très longues,
- ne lisent pas l'anglais car dans de nombreux cas elles ne sont pas traduites,
- Ou encore ne comprennent pas les tournures juridiques.

Tout est fait pour que l'utilisateur ne comprenne pas précisément ce qu'il télécharge ou pour qu'il ne le voie pas. En outre de nombreux logiciels gratuits ne fonctionnent plus si les spywares sont désinstallés. La réciproque, elle, est fausse, puisque les spywares restent actifs même après la désinstallation du logiciel qui les contenait.

Mais les éditeurs, dès lors que la mention est faite (même incompréhensible ou très bien cachée…), ne peuvent plus être considérés en infraction avec la loi.

Quelques exemples de EULA (End User License Agreement) :

"KaZaa reserves the right to change or modify any of the terms and conditions of this licence and any of the policies governing the Software at any time in its sole discretion without direct notice to you. Your continued use of the software following these changes will constitute your acceptance of such terms."

« Kazaa se réserve le droit de changer ou modifier tout terme et condition de cette licence et toute politique régissant le logiciel à tout moment sans en avertir directement l'utilisateur. Continuer à utiliser le logiciel après ces changements sera considéré comme l'acceptation de ces nouveaux termes. »

"Your hereby grant BDE the right to access and use the unused computing power and storage space on your computer/s an/or internet access or bandwidth for the aggregation of content and use in distributed computing. The user acknowledges and authorized this use without the right of compensation."

"Par la présente vous autorisez BDE à utiliser l'espace et la puissance disponibles de votre ordinateur et/ou la bande passante de votre accès à Internet pour l'agrégation de contenu et l'utilisation en système distribué."

La visionneuse de BDE (Brillant Digital Entertainment) agit comme un cheval de Troie. Cette visionneuse a été distribué en 2001 à travers de réseau de peer to peer : Kazaa et Morpheus.

BDE justifiait l'utilisation d'espace, de puissance et de bande passante ne lui appartenant pas, pour la création d'un réseau privé. Altnet, société appartenant à BDE (qui s'est rapprochée de Double Click que nous verrons plus loin) a déclaré :

« Des millions d'ordinateurs sont connectés à chaque instant sur Internet chacun avec des réserves en puissance de calcul, capacités de stockage et bande passante inutilisée. A travers Altnet, nous allons créer un réseau privé de type peer-to-peer pour permettre à nos clients d'accéder et d'utiliser ces excès de puissances de calcul, de capacités de stockage et bande passante inutilisée, pour diverses applications. »

Ces programmes permettent donc une utilisation à distance des ressources de l'ordinateur sur lequel ils sont installés.

1.7/ La détection et les contre-mesures

1.7.1. Prévention

Il est utile d'avoir un firewall et un anti-virus même s'ils ne sont pas fiables à 100% (ports ouverts, mise à jour pas encore en place…), ils réduisent déjà les risques.

Lire avec attention les conditions d'utilisation des logiciels qu'on télécharge et ne pas installer les programmes supplémentaires sans savoir précisément à quoi ils servent et ce qu'ils sont.
Lire les chartes de respect de la vie privée ou clauses de vie privée de l'entreprise en question et faire très attention si celles ci sont vagues.

Pour réduire les informations transmises il peut être intéressant de dédier un ordinateur à la messagerie, un autre à la navigation… lorsqu'il est possible de le faire. On réduit ainsi les informations transmises à ce qu'il y a sur l'ordinateur.

Et bien sûr donner le moins possible d'informations personnelles sauf quand cela est vraiment indispensable.

Un logiciel de cryptographie permet une sécurité supérieure.

1.7.2. La détection et l'éradication

- Grâce à une liste des spywares on peut repérer le programme et le supprimer.

- Grâce à un firewall : en repérant les paquets sortants non autorisés ou qui ne correspondent à aucun programme que l'on connaît. Mais si le spyware est interne à un programme utilisé on ne pourra pas le repérer de cette manière.

- Pour les spywares logiciels, n'étant pas des virus, les antivirus ne les détectent pas et ce n'est pas leur rôle.

- Les logiciels spécialisés en détection et destruction des spywares dont ceux spécialisés pour les BHO : ad aware de Lavasoft, Pest Pastrol (détecte les trojans et les spywares), X-cleaner, spyboot search & destroy, BHO Cop (détecte les BHO).

1.7.3. Le P3P : Platform for Privacy Preferences Projet

Consortium du World Wide Web pour une plate-forme d'expression de choix en matière de respect de la vie privée et standard d'établissement de profils ouverts.

Depuis 1997, les grandes firmes informatiques américaines ont développé, sous l'égide du W3C (World Wide Web Consortium), un standard dit P3P (Platform for Privacy Preference) pour encadrer la réutilisation par les sites des profils électroniques des internautes.

Les technologies Passport (Microsoft), Magic Carpet (AOL) ou Liberty Alliance (Sun Microsystems) sont les premières applications industrielles du P3P. Elles organisent l'échange automatique des données personnelles sur le Web, en fonction du consentement de l'internaute.

Ces technologies doivent permettrent d'éviter l'enregistrement à répétition et de choisir le niveau de protection des données privées.

Les régies publicitaires, en plus des espiogiciels, utilisent aussi d'autres technologies qui ont à l'origine une autre raison d'être, soit directement (les spywares récupèrent les informations données par ces différentes technologies), soit comme moyen autre que le logiciel espion.

Souvent il y a conjonction de plusieurs techniques simultanées (cookies plus autres informations qui permettent des recoupements…) qui n'ont pas comme but originel la récupération d'informations personnelles. Ce sont ces technologies que nous verrons dans un deuxième chapitre.

II / Les Codes Malicieux utilisés comme mouchard : Les chevaux de Troie (trojan horse ou trojan)

Définition du NIST (National Institute of Standards and Technology) : un cheval de Troie est un programme qui exécute une tâche souhaitée, mais inclut aussi des fonctions inattendues et indésirables. La différence avec un virus est qu'il ne se réplique pas automatiquement et n'affecte normalement pas les fichiers contenus dans l'ordinateur.
(Virus : segment de code auto reproducteur qui doit être attaché à un hôte exécutable. …)

Ce sont à l'origine de simples programmes destinés à faire effectuer des actions à un ordinateur à l'insu de l'utilisateur.

Ce terme s'applique aujourd'hui davantage aux applications de capture de données, bien qu'ils aient à l'origine comme but la destruction ou le détournement de données. En effet tous les chevaux de Troie ont une fonction commune : donner accès à des données contenues dans un système. C'est pour cela que le cheval de Troie est le mouchard par excellence car il est fait pour récupérer des données le plus discrètement possible. C'est aussi pour cette raison que certaines personnes ont qualifié les espiogiciels de chevaux de Troie légaux, car ils en ont toutes les caractéristiques.

Leur objectif est d'ouvrir une porte dérobée (backdoor) sur le système cible, permettant ensuite à l'attaquant de revenir épier, collecter des données ou contrôler le système. Certains sont même devenus des outils d'administration à distance.

Contrairement au virus, ils sont beaucoup plus faciles à utiliser et donc accessibles à un plus grand nombre de personnes. C'est en réalité le moyen le plus simple de piratage.

Mais il existe aujourd'hui des vers très dangereux qui contiennent un cheval de Troie : c'est le cas du vers Bugbear.

2.1/ Principe

Pour s'introduire, le cheval de Troie utilise toutes sortes de moyens :

- Il peut s'implanter directement en exploitant les failles de sécurité d'un système ou d'un logiciel/
- Être contenu dans un programme comme un économiseur d'écran, un jeu…
- Être téléchargé involontairement sur un site web ou ftp.
- Être installé sur la machine par une personne y ayant physiquement accès.
- Par une pièce jointe d'un e-mail…

Une fois introduit, il se cache dans des répertoires système ou se lie à des exécutables.
Il modifie le système d'exploitation de manière à pouvoir démarrer en même temps que la machine. Sous Windows c'est la base de registre.

2.2 / Classification

En plus de permettre la récupération d'information sur l'ordinateur, ils ont souvent une fonction key logger qui leur permet d'enregistrer toutes les frappes au clavier et aussi une fonction capture d'écran. Ils ont également toute une série de fonctions comme éteindre et redémarrer l'ordinateur (séquences de reboot), bloquer le clavier, démarrer des applications, ouvrir des documents, récupérer les mots de passe…

En fonction des différentes fonctions dont ils disposent on peut les classer en quatre sortes :

- les RAT : les chevaux de Troie télécommandés ou d'administration à distance (Remote Access Trojan ou Remote Administration Trojan)
- les chevaux de Troie FTP (File Transfert Protocole)
- les chevaux de Troie de mots de passe (passwords trojan)
- les enregistreurs de touches ou key loggers.

2.2.1. Les chevaux de Troie d'administration à distance (RAT)

Ce sont les chevaux de Troie les plus courants mais aussi les plus dangereux. Ils permettent de faire absolument toutes les opérations que l'utilisateur devant son ordinateur peut faire : ainsi avec un RAT on peut lire, modifier, télécharger tout fichier présent sur l'ordinateur cible et en télécharger sur l'ordinateur cible, récupérer tous les mots de passe et autres, modifier le système…

Un RAT créé une brèche dans l'ordinateur en ouvrant clandestinement un port réseau, ils sont par extension aussi appelés backdoor (porte dérobée). Ils ont une structure client / serveur, c'est à dire deux programmes distincts : le programme serveur doit être placé sur l'ordinateur cible et le programme client permet l'accès au dit ordinateur en communiquant avec le programme serveur implanté et totalement clandestin. Ils nécessitent donc une connexion internet.

Les plus connus sont Backorifice et Netbus.

2.2.2. Les chevaux de Troie FTP

Ils sont assez proches des RAT mais ils n'ont pas autant de fonctionnalités. Ils utilisent également une porte dérobée (backdoor) et ont aussi une structure client serveur. Par contre leur particularité est qu'une fois le serveur installé, ils fonctionnent comme un serveur FTP classique qui permet donc le transfert de fichier. Le programme client n'est donc plus spécifique au cheval de Troie, tout client FTP permet l'accès au serveur. Mais les opérations possibles sont forcément réduites à ce que permet un serveur FTP, c'est à dire surtout des interventions sur les fichiers, et ils nécessitent bien sûr que la machine cible soit connectée à Internet.

Ils sont moins connus que les RAT mais aussi moins détectables. En outre ils utilisent en général le port FTP 21, qui est un port commun (certains peuvent être paramétrés pour utiliser un autre port).

2.2.3. Les chevaux de Troie de mots de passe

Ils vont chercher les mots de passe qui ont été stockés sur un ordinateur, lorsque l'utilisateur a demandé à ce qu'ils soient retenus. Certains sont spécialisés dans la recherche de mots de passe de logiciels bien définis, d'autres récupèrent tous les mots de passe.

Il y a deux types de récupération de ces mots de passe :

- soit en mode local, c'est à dire qu'il faut avoir accès à la machine cible et appeler le programme qui affiche alors les mots de passe trouvés,
- soit en mode distant, tous les mots de passe trouvés sont envoyés sur une boite e-mail et transitent par le serveur de la boite mail du destinataire et non pas directement comme pour les autres chevaux de Troie. Il n'y a pas de programme client, il suffit juste de configurer le programme serveur (avec la boite mail) avant de l'implanter.

Ils ne sont pas actifs en permanence. En général ils ne fonctionnent qu'une fois, à l'exception de certains qui peuvent redémarrer lorsque certains mots de passe sont modifiés. D'autres ont une fonction de destruction une fois les mots de passe envoyés.

Leur intérêt par rapport aux RAT qui ont aussi cette fonction là, est que ce sont des programmes beaucoup plus légers et moins repérables.

2.2.4. Les enregistreurs de touches ou key loggers.

Ce sont des enregistreurs d'activités informatiques permettant d'enregistrer les touches pressées par un utilisateur sur son clavier et tous les événements déclenchés.

Ils ne sont pas toujours considérés comme chevaux de Troie mais leur fonction étant la récupération d'information, ils correspondent tout à fait au type « trojan ». L'enregistreur de touche peut soit être installé seul et n'avoir pas d'autre fonction, soit être une des fonctions d'un cheval de Troie plus développé, de la même manière que les chevaux de Troie de mots de passe.

Ils permettent simplement l'enregistrement d'informations mais ne modifient rien sur la machine cible. Ils vont permettre de récupérer tous les mots de passe, identifiants… qui ont été tapés au clavier. Ils se lancent automatiquement au démarrage de l'ordinateur.

Il y a trois sortes de key loggers en fonction de la technique de récupération des informations :

- mode local : les informations généralement cryptées dans un fichier log ou plusieurs fichiers log (cela dépend du key loggers) sont ensuite récupérées directement sur l'ordinateur cible : dans ce cas l'enregistreur de touches a aussi été mis manuellement sur l'ordinateur.
- les e-mails key loggers : ils envoient périodiquement les informations à une adresse mail configurée préalablement.
- Les Remote key loggers (mode distant) : ils nécessitent un programme client et permettent, soit de voir directement la saisie à l'écran, soit de se connecter régulièrement au serveur pour récupérer les informations qui sont alors enregistrées temporairement.

De la même manière que les chevaux de Troie de mots de passe, ils sont beaucoup plus petits que les RAT et moins repérables.

2.3 / Les différentes utilisations des chevaux de Troie

Des programmes d'enregistreurs de touches ont été commercialisés pour des utilisations personnelles ou pour des utilisations en entreprise. Ces programmes étant autorisés, ils ne sont pas repérés par les logiciels de détection.

Les chevaux de Troie ne sont donc pas utilisés qu'à des fins de piratages mais dans ce cas ils peuvent avoir une autre dénomination :

- Le FBI depuis les attentats du 11 septembre 2001 utilise un cheval de Troie appelé Magic Lantern ou Lanterne Magique qui est un key logger. Il est reçu par courrier électronique et ouvre ensuite une porte dérobée (backdoor). Il doit les aider à traquer les terroristes potentiels mais permet surtout d'identifier les mots de passe et les clés des programmes de cryptage. Le FBI a démenti disposer d'un tel outil mais a reconnu travailler sur sa conception.

- On les trouve en usage personnel comme moyen de surveillance (pour les enfants, les maris jaloux…).

- Ils se développent de plus en plus dans les entreprises pour contrôler le travail des salariés : ils sont appelés logiciels de télé-maintenance.

Sur ce dernier point le Code du Travail en France exige que le salarié, dont le travail est vérifié par un système de ce genre, soit prévenu avant que le système soit mis en place, c'est le principe de transparence :

« Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi. »
Article L121-8 (inséré par Loi nº 92-1446 du 31 décembre 1992 art. 26)

De plus, le contrôle doit également être justifié par la nature des tâches et proportionné au but recherché. La proportionnalité est une affaire de cas par cas car elle dépend du degré de sécurité et de surveillance exigée par l'entreprise.

Le troisième point est que la mise en place de ce contrôle doit faire l'objet d'une discussion collective :
« Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »
Article L432-2-1 (Loi nº 2001-152 du 19 février 2001 art. 1)

Au niveau européen une recommandation du comité des ministres du Conseil de l'Europe du 18 janvier 1989, imposait en substance ce qui a été retranscrit dans la loi 92-1446 mais en précisant que l'accord du salarié devrait être recherché lorsque « *la procédure de consultation … révèle une possibilité d'atteinte au respect de la vie privée et de la dignité humaine des employés… ».*

2.4/ Détection et éradication

- La plupart de ces dispositifs peuvent être détectés par des antivirus mais pas tous.
- Des logiciels spécialisés existent ainsi que des programmes spécifiques pour chaque cheval de Troie.
- On peut les détecter grâce à un ralentissement du système au démarrage mais ce n'est en général pas très visible.
- Des listes de chevaux de Troie et des ports qu'ils utilisent sont mises à jour régulièrement et peuvent aussi permettre certaines vérifications.
- Il peut être intéressant d'effectuer une analyse des ports (scan ports) de manière à voir ceux qui sont ouverts, et de les fermer ou les protéger.
- On peut également les repérer avec un pare feu, si des ports inhabituels sont ouverts. Certains utilisent les ports communs. Dans ce cas on peut voir qu'un programme inconnu cherche à communiquer à l'extérieur. Le pare feu peut également servir à bloquer la communication entre le serveur et le client (pour les chevaux de Troie utilisant ce principe).
- On peut les supprimer manuellement. Dans ce cas il faut supprimer le programme et faire en sorte que le programme ne soit plus activé au démarrage (trouver la clé dans la base de registre ou celle qui a été modifiée…)

Il est aussi très important d'effectuer régulièrement les mises à jour et correctifs des systèmes d'exploitations et des logiciels, les chevaux de Troie utilisant des trous ou failles de sécurité. On réduit ainsi les risques d'infection. Les utilisateurs ne sont pas suffisamment sensibilisés à l'importance des correctifs, c'est pour cela qu'on retrouve des chevaux de Troie encore actifs alors qu'ils utilisent des failles corrigées depuis longtemps.

III / Les réseaux d'espionnage d'États ou les systèmes de surveillance et d'interception électronique

« Le respect du secret des correspondances doit faire l'objet de conciliation avec d'autres principes tout aussi important comme l'ordre public et la sécurité nationale. Donc certaines atteintes sont permises à l'encontre de ces droits mais seulement dans certains buts et si celles ci sont légales. »

Ainsi les réseaux d'espionnage d'état sont justifiés par des raisons d'ordre public, de lutte contre la criminalité…, de sécurité dans un sens large.

L'interception des signaux est appelée internationalement SIGINT pour Signal Intelligence. Ces systèmes, utilisés depuis l'invention de la radio, permettent de capter tous les signaux. Ils effectuent l'interception secrète des communications étrangères, appelé COMINT (Communication Intelligence). La NSA le définit comme « l'ensemble des informations techniques et des renseignements détournés des communications étrangères par une autre voie que le médium ordinaire ».

L'organisation UKUSA est un pacte de sécurité créé à l'origine pour intercepter les communications politiques et militaires du bloc soviétique. Le pacte UKASA a été signé par les Etats Unis et le Royaume Uni en 1947. Il a ensuite été élargi au Canada qui a signé un accord bilatéral avec les Etats Unis, le CANUSA agreement, puis à la Nouvelle Zélande et l'Australie.

Le système fait donc appel aux services de renseignements spécifiques des cinq pays participants :

- la NSA (National Security Agency) aux Etats Unis,
- le GSHQ (Government Communications Headquarters) au Royaume Uni
- le DSD (Defense Signals Directorate) en Australie,
- le CSE (Communication Security Etablishment) au Canada,
- le GSCB (Government Communications Security Bureau) en Nouvelle Zélande

Ses attributions sont montées en puissance quand a été mis en place le réseau Echelon dans les années 70. Cette organisation est restée longtemps secrète, ce n'est que récemment qu'elle a été indiquée dans des rapports officiels.

3.1/ Le système Échelon

A l'origine système à finalité militaire, mis en œuvre après guerre pour contrer la menace soviétique, c'est aujourd'hui un système d'interception mondial des communications privées et économiques : il permet d'intercepter toutes les communications à partir de mots clés dits « sensibles ».

En effet le système n'a pas été conçu pour intercepter seulement certains types de communications, comme les messages à caractère militaire lors de la guerre froide, mais il a eu vocation à intercepter de manière indistincte tous les messages dans le monde, quels que soient la nature de leur support et leur contenu, c'est-à-dire y compris les communications privées.

Le réseau planétaire de surveillance Echelon a été créé en majorité par la NSA, elle en est le maître d'œuvre et les États Unis ont une position dominante dans le pacte. La NSA couvre tout le champs des technologies de l'information militaire et civile et est chargée du contre espionnage, de la protection des communications gouvernementales et militaires.

La NSA a été soupçonnée de vendre des informations de veilles économiques et documentaires aux grandes sociétés américaines, ce réseau servirait actuellement à espionner des données commerciales.

Son existence est devenue publique en 2000 mais révélée pour la première fois en 1998 par un rapport commandé par le parlement européen à la STOA (Scientific and Technological Options Assessment) grâce à la déclassification de documents secrets par la NSA.

Il a été critiqué par de nombreux groupes privés comme l'EPIC (Electronic Privacy Information Center). Une association française a porté plaindre contre le système Echelon le 23 mars 2000. Elle a porté plaindre contre X devant le Tribunal de Grande Instance de Paris (la plainte s'effectuant contre les gens qui l'utilisent et non pas contre le système).

Le Parlement Européen a reconnu la nécessité de systèmes de surveillance électronique mais a demandé plus de transparence et des systèmes de contrôle démocratiques.

3.1.1. Principe et fonctionnement

Projet de surveillance globale des communications sur l'Internet, le principe est de détourner un programme de détection des intrusions, Fidnet, à des fins d'interception globale. Un réseau de stations d'écoute a été établi au niveau mondial afin d'intercepter les communications par satellites, les communications terrestres ou même radio.

Le fonctionnement du réseau Echelon comporte trois phases : l'écoute des télécommunications, le traitement des informations recueillies et l'échange des données.

- Les méthodes d'écoute concernent tous les vecteurs utilisés pour les communications modernes : ondes radio, satellites, câbles terrestres ou sous-marins, fibres optiques, réseaux informatiques…

Ainsi dans une station d'écoute d'un pays du pacte, tous les signaux numériques et analogiques sont captés. Pour capter ces différents signaux plusieurs techniques sont utilisées : les satellites de la NSA, interception des signaux électriques grâce aux répétiteurs, interception et filtrage des paquets sur Internet. Cisco Systems avait été mis en cause pour l'installation de mouchards à la demande de la NSA dans certains de ses routeurs Internet.

Ils sont amplifiés puis triés mais aussi analysés car les messages qui ne sont pas en langue anglaise doivent être traduits.

- Des ordinateurs de type Super-Gray traitent et analysent en temps réel les informations recueillies en se servant d'un dictionnaire qui contient des mots clés. Un logiciel nommé Oratory va ensuite repérer automatiquement les messages contenant ces mots clés.

Chaque station possède son propre dictionnaire afin de mieux coller avec l'environnement local. Toutes les transmissions repérées de cette manière sont conservées, cryptées puis envoyées aux Etats-Unis.

- Au siège de la NSA les messages sont décryptés, analysés et classés.

Les données traitées sont ensuite retournées aux pays intéressés sous forme de rapports ou de notes succinctes.

La NSA possède des stations d'écoute au Danemark, aux Pays Bas, en Angleterre, en Allemagne, en Norvège, en Suède, en Suisse, au Japon…

3.1.2. Les doutes sur l'espionnage économique

Le gouvernement américain n'a pas totalement démenti les écoutes dans un intérêt commercial. L'accusation d'espionnage économique fait de nombreuses fois au système Echelon a été plus ou moins prouvé lors d'affaires telles que Thomson-CSF contre Raytheon pour un marché de radars au Brésil, Airbus contre Boeing en Arabie Saoudite, ou la firme allemande Siemens pour un marché d'électronique en Inde.

Les Etats-Unis ont répondu à ces accusations en précisant qu'ils intervenaient uniquement pour moraliser le commerce international et éviter ainsi que les entreprises américaines soient pénalisées par des comportements délictueux de leurs concurrents. Ainsi le directeur de la CIA affirmait que « l'agence intervient lorsqu'une entreprise américaine pourrait être «lésée» dans ses intérêts par un concurrent ne se conformant pas à des pratiques loyales. »

3.1.3. Le problème des libertés individuelles : les atteintes à la vie privée

Des associations pour la défense de la vie privée se sont insurgées, mais l'Etat américain affirme qu'il n'écoute pas les conversations privées et qu'il respecte les lois américaines. Pourtant un simple soupçon permet d'écouter les communications d'un individu.

Aux Etats-Unis, la protection des citoyens est assurée par le quatrième amendement. Celui-ci affirme que « *le droit pour le peuple d'être protégé... contre des perquisitions et saisies déraisonnables ne devra pas être violé.* » Les activités des agences américaines sont soumises à cet amendement.

3.1.4. Les limites du système Échelon

Les réseaux filaires restent difficiles à intercepter sans que l'utilisateur ne s'en aperçoive ou sans la complicité de l'opérateur de réseau. L'interception à partir de fibres optiques serait ainsi délicate en raison de la nécessité de se placer au niveau d'un répétiteur qui amplifie le

signal lumineux à intervalles réguliers et du fait que toute intrusion sur la fibre optique est décelée en bout de ligne. Mais certains experts affirment que cela est possible.

Un des problèmes que rencontre actuellement la NSA est les communications cryptées. Elle doit suivre l'évolution de la cryptographie de manière à pouvoir continuer à analyser les communications. En outre les communications cryptées demandent d'énormes capacités de calcul. Mais c'est également une des seules alternatives face à ce système pour les entreprises et les gouvernements afin d'éviter des fuites d'informations de type économiques ou politiques.
Le Parlement Européen a d'ailleurs étudié dans plusieurs rapports les possibilités de chiffrement et de cryptographie et les lois en vigueur dans les différents pays pour contrer ces risques (lien vers les rapports dans la bibliographie).

La traduction des messages surtout lorsqu'ils sont dans des langues plus rares et la multiplication du nombre de communications posent aussi un problème de capacité d'analyse mais aussi de stockage. La NSA semble régresser en capacité.

3.2/ Carnivore ou DCS1000

Carnivore est un système utilisé depuis environ 1999 par le FBI et installé chez les fournisseurs d'accès américains pour capturer des données véhiculées sur Internet. Il a changé de nom en 2001 est s'appelle aujourd'hui DCS1000 (Digital Collection System). Ce programme est à l'échelon national.

C'est un programme mis en place par le FBI depuis 1997 afin de surveiller les communications électroniques de personnes suspectées de crimes.
Le premier système s'appelait Omnivore. En 1999, le programme devient Carnivore.

3.2.1. Historique du projet et validité vis à vis de la loi

C'est le Wall Street Journal du 11 juillet 2000 qui a dévoilé le programme Carnivore, suite au révélations de l'avocat d'Earthlink, 2ème FAI aux Etats Unis. Le FBI avait installé sur les serveurs d'Earthlink un système nommé Etherpeek qui était censé enregistrer les communications d'un seul abonné. Or il s'est avéré qu'il enregistrait toutes les communications. Les associations de défense pour la vie privée se sont saisies de l'affaire notamment l'EPIC (Electonic Privacy Information Center) et l'ACLU (American Civil liberties Union). Mais le FAI a été ensuite contraint par la loi d'installer Carnivore.

En effet cette surveillance a été définitivement légalisée avec l'adoption par la Chambre des représentants américains du « USA-Patriot Act » (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism), le 24 octobre 2001, d'une loi qui confirme l'autorisation accordée au FBI de brancher le système Carnivore sur le réseau d'un fournisseur d'accès. Ceci dans le but de surveiller la circulation des messages électroniques et de conserver les traces de la navigation sur le Web d'une personne suspectée de contact avec une puissance étrangère.

3.2.2. Principe

C'est un programme qui fonctionne comme un sniffer spécialisé, capable de filtrer des paquets de données, qui transitent entre l'utilisateur et le FAI. Un logiciel est installé chez le fournisseur d'accès.

Il utilise des filtres prédéfinis en fonction de la nature de l'écoute, filtres qui peuvent être modifiés à distance sans que le FAI le sache. Il s'intéresse à toutes les formes de communications numériques (correspondances, fax…) et de communications internet. Il peut en effet suivre tout le parcours d'un internaute sur la toile. Il vient plus ou moins en complément d'Echelon qui est plus porté sur les communications de types analogiques ou numériques.

3.3/ Les autres projets d'états

3.3.1. Suisse : Satos-3

Le financement de ce projet a été adopté en 1999 par les Chambres Fédérales. Ce projet doit permettre d'intercepter d'ici à 2004 toutes les communications et transferts de données (fax, e-mail, télex, téléphone) qui transitent par satellite.

Ce système serait semblable à Echelon et devrait disposer d'une dizaine de paraboles d'écoute fonctionnant avec un logiciel de recherche et traitement de mots clés.

Les justifications de ce projet sont la lutte contre le terrorisme international, le crime organisé, et l'espionnage industriel. Légalement seules les communications à l'étranger pourront être interceptées.

3.3.2. France : surnommé Frenchelon par les anglo-saxons

Système de surveillance construit par la DGSE (Direction Générale de la Sécurité Extérieure) et par la DRM (Direction du renseignement militaire).
Le projet Essaim est un système spatial d'écoute SIGINT, système de quatre microsatellites. Il permettra de surveiller l'activité radio et radar. Son lancement est prévu pour 2004. C'est un projet géré par la DGA.

Mais les moyens actuels français sont géographiquement orientés et limités et ne peuvent donc pas être comparés au réseau Échelon.

3.3.3. Russie : Sorm-2 (System of Efficient Research Measures)

Système de procédures opérationnelles d'enquête. Il a pour but de surveiller l'Internet russe. Le principe est de placer une « boite » chez tous les fournisseurs d'accès russes qui achemine le trafic électronique jusqu'au siège local des services de sécurité, le FSB (ex-KGB).

3.3.4. Les autres pays

L'Angleterre a également un équivalent de Carnivore appelé M15, qui est installé chez les FAI et relié directement au service secret anglais.

Au Japon le système s'appelle « Tempory Mail Box » ou « Kari-no-mail », similaire à Carnivore.
On pourrait aussi citer l'Inde, la Pologne, la Hollande, la Norvège (VDI) et beaucoup d'autres.

Dans la plupart de ces pays l'installation de ces différents systèmes devait être financée par les fournisseurs d'accès à Internet.

La Commission Européenne s'est également posée la question de la création d'un réseau européen d'interception des communications.

3.4/ La législation française sur le sujet

« Le secret des correspondances émises par la voie des télécommunications est garanti par la loi.
Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. »
(Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, article 1er)

« Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des télécommunications ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisée et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées.
(Titre II : des interceptions de sécurité, Art. 3)

« Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation des fins mentionnées à l'article 3. (...) »
(Art. 12)

Ces systèmes utilisent donc beaucoup de technologies détournées à des fins autres, de la même manière que les spywares logiciels et les chevaux de Troie. C'est ce que nous allons étudier dans un deuxième chapitre.

Utilisations détournées, abusives de ressources normales

2ème chapitre

Ce sont les abus de solutions matériels ou logiciels (logiciels normaux et non malveillants pour en faire une utilisation malveillante). Toute ressource informatique peut être utilisée de manière abusive : systèmes d'exploitation, applications, services. De nombreuses techniques créent des traces bien que n'étant pas conçues pour faire de la surveillance et ces traces peuvent ensuite être réutilisées à des fins de profilage.

Certaines techniques peuvent être considérées comme mouchard informatique à elles seules mais peuvent aussi être utilisées par des spywares logiciels. Ce sont les différentes techniques d'identification des internautes, la première étant l'adresse IP.

De nombreuses traces peuvent être trouvées sur un disque dur et peuvent ensuite permettre d'établir des profils.

Le système d'exploitation, le navigateur et les différents logiciels utilisés conservent des traces du travail effectué :

- les fichiers de log,
- les fichiers de travail temporaires (.tmp),
- les fichiers de copies intermédiaires (.bak),
- les dernières adresses de pages Web consultées,
- les listes de saisie rapide
- Les fichiers de cache du navigateur ou Temporary Internet Files : garde en mémoire les sites et les pages fréquemment visités pour désengorger le réseau (optimise les temps de chargement, même rôle qu'un proxy),
- Les fichiers index.dat de Windows
- La liste des documents récemment manipulés sous Windows
- La base de registre : nom, adresse e-mail, numéro de série de Windows… Peut être lu par un VBscript ou un Active X inclut dans une page web.

De plus l'information transite à travers de nombreuses infrastructures réseau : on peut alors se poser au centre de ces structures pour récupérer des informations.

Des traces sont gardées à plusieurs niveaux même après la suppression d'un fichier du disque dur : sur le dispositif de sauvegarde ou miroir à l'intérieur d'une entreprise, sur les serveurs de messagerie et autres, sur les proxies, les pares feu, les fournisseurs d'accès Internet (FAI).

Cette partie regroupe donc des choses très différentes :

- Des techniques utilisées par les spywares dédiés mais détournées de leur but originel ou des techniques de sécurité ou de fonctionnement classique mais pouvant être utilisées pour récolter des informations : les Guid, cookies et web bugs, les logs, quelques technologies dangereuses comme les active X, les scripts CGI, les technologies sans fil.

- Des projets à la limite du spyware dont les justifications sont toutes autres, mais qui dans leur fonctionnement peuvent le devenir. Des projets légaux donc.

I / Guid (Global Unique Identifier)

Numéro permettant d'identifier de manière unique et certaine un composant matériel ou logiciel d'un ordinateur ou l'ordinateur lui-même.

- Lors de l'enregistrement en ligne de Windows un Guid est attribué ayant une valeur numérique de 32 chiffres (**le MSID : Microsoft ID**) dont les 12 derniers sont l'adresse MAC de la carte Ethernet. Il est envoyé par un active X. C'est ce code qui est ensuite incorporé dans les documents Word, Excel…

- **Hardware ID ou HWID : numéro d'identification matériel**. Envoyé à Microsoft si l'utilisateur le souhaite (renseignements sur les différents matériels et certains logiciels). Mais en raison d'un bug (raison officiel) ce numéro était envoyé automatiquement sans l'accord de l'utilisateur (présent sur Windows 98 et 2000 et les versions 4 et 5 d'Internet explorer). C'est ce numéro qui a été appelé par certains le mouchard de windows. De plus ce guid mis dans un cookie était ensuite envoyé sur le site de microsoft. La raison invoquée, était qu'il simplifiait le travail de l'équipe d'assistance téléphonique.

- **MAC (Media Access Control) Adress** : guid matériel unique contenu dans les cartes Ethernet. Norme IEEE 802 qui date de 1970, adresse liée à un code unique. Adresse IP.

- **Numéro de processeur avec le Pentium III** : numéro d'immatriculation inscrit en dur dans la mémoire de la puce, c'est un numéro de série unique de 96 bits appelé PSN (Processor Serial Number) qui était tatoué sur la puce.

  La justification de ce numéro était qu'il faciliterait le commerce électronique, la protection des contenus et éviterait la fraude. Mais ce numéro allait à l'encontre des protocoles européens concernant la sécurité, il fut donc interdit et un logiciel a été mis en ligne permettant de le désactiver sous Windows… Mais certains doutent de son efficacité…
  Ce tatouage concernait les Pentium mais aussi les processeurs Celeron.
  Ce numéro permettait d'identifier la machine et cette affaire s'est produite à peu près en même temps que celle de mouchard de Windows 98 qui lui identifiait l'utilisateur…

- Le bios contient aussi un Guid.

- Toutes les cartes en ont un : cartes mères, cartes graphiques, carte réseau…

- Les logiciels installés : numéro de série, de licence et en particulier sur Word et Excel 97 et 2000. Ce numéro a également été nommé le mouchard de Microsoft Office. En effet le MSID était incorporé dans les documents office, on pouvait donc remonter jusqu'à l'ordinateur qui avait produit le document.

- Le CLSID (Class Identifier) : numéro d'identification situé dans la base de registre attribué à chaque objet. Référencement de chaque composant qu'il soit matériel ou logiciel.

Ainsi les Guid font partie des technologies pouvant être utilisées par les spywares ou même devenir par eux-mêmes des mouchards selon l'utilisation qui en est faite. En effet ils permettent de définir précisément un ordinateur et par recoupement son utilisateur. Le rapprochement entre l'ordinateur et l'utilisateur peut être très facilement fait grâce au nom et à l'adresse donnés pour un enregistrement quelconque ou dans un message… Les Guid sont ainsi utilisés par les spywares logiciels de manière à reconnaître de manière certaine un individu. Ils deviennent alors un outil de profilage.

Ce numéro peut ainsi permettre de profiler quelqu'un, en particulier avec les Guid qui étaient (ou sont ?) contenus dans les fichiers Word et Excel. Les Guid sont un moyen rêvé d'espionnage. Ils ont permis de retrouver des auteurs de virus très facilement. S'ils permettent d'identifier des individus néfastes ils peuvent identifier tout individu…

Les Guid logiciels doivent permettre d'éviter la contre-façon : on arrive sur la même problématique du TCG que l'on verra plus loin, sur la limite entre vie privée et technologie anti-fraude ou sécuritaire.

II / Les Cookies et Web bugs

Nous utiliserons ici plus facilement les termes anglais car ce sont les plus couramment employés tout en précisant leur nom dans la langue française.

2.1 / Les cookies (ou témoins de connexion)

Un cookie est un fichier téléchargé sur le poste d'un internaute par le serveur Web qu'il visite et qui contient plusieurs informations qui peuvent être récupérées ultérieurement. Ils sont stockés sur le disque dur de l'utilisateur temporairement ou de façon quasi permanente. Leur technique repose sur le protocole http donc seul un serveur Web peut en envoyer.
Ils ont été inventés en 1995 avec la version 2 de Netscape. Ils sont destinés à rendre la navigation sur Internet plus facile et plus rapide. Les cookies mémorisent différentes informations de l'utilisateur telles que ses préférences sur un site, des réponses à des questions permettant d'accéder directement à la page suivante d'un site, un mot de passe si l'on a demandé au navigateur de s'en souvenir, d'autres données personnelles ou confidentielles, un Guid…

2.1.1. Fonctionnement

On distingue les cookies de session et les cookies rémanents :

- Les cookies de session ne contiennent pas de date d'expiration et sont automatiquement détruits lorsque l'internaute ferme la session ouverte sur le site Internet. Ils sont généralement créés pour des raisons techniques et n'ont pas pour objectif d'instaurer un lien permanent entre la machine de l'internaute et le site Internet consulté.

- Les cookies rémanents contiennent une date d'expiration fixée par leur auteur et sont destinés à permettre au serveur Web d'accéder aux informations qu'il contient jusqu'à son échéance.

Leurs formats garantissent plusieurs points :

- Ils sont purement passifs (fichier texte), ne peuvent pas contenir de virus et ne peuvent pas faire accomplir d'action à une machine.
- Ils ne peuvent pas collecter d'informations sur un ordinateur et ne permettent pas d'y accéder.
- Ils ne peuvent normalement être lus que par le serveur web qui les a écrit.

Il y a plusieurs façons de gérer les cookies : en faisant appel au javascript ou VBscript, soit au moyen de programmes CGI.

2.1.2. Utilisation

La plupart des sites s'en servent pour faire des calculs de statistiques, pour justifier le passage des internautes,… C'est un outil supplémentaire de gestion de sites qu'ils soient commerciaux ou non.

De plus le cookie est le moyen le plus simple pour tous les sites qui demandent une identification (messagerie…). En effet le http ne gère pas la notion de session. Dans ce cas le cookie n'est qu'un simple outil technique pour assurer une session.

Malheureusement leur utilisation peut être détournée et ils peuvent alors être utilisés par des logiciels spywares ou en devenir en raison de l'utilisation qui en est faite. Le cookie peut aussi servir à faire du traçage et du profilage :

- Les spywares peuvent récupérer ces cookies afin de lire les informations, pour certaines confidentielles.
- En lisant les noms des cookies on peut effectuer un profilage de la personne.
- Le Guid inséré dans le cookie permet d'identifier que tel ordinateur est allé sur tel site.
- Les régies publicitaires s'en servent pour déterminer des profils : en insérant un cookie qui sera reconnu sur certains sites et qui permettra après recoupement des informations d'établir un profil.
- Par le biais d'un croisement de bases de données, les cookies rémanents peuvent être «recoupés » avec des données nominatives, de telle sorte que ces données nominatives sont associées au profil – anonyme – défini dans les cookies, sans le consentement de l'Internaute sur l'ordinateur duquel ces cookies sont enregistrés. L'analogie entre un ordinateur et une personne physique est assez difficile à faire (cybercafés ou ordinateur familial…) mais cela a déjà été réalisé.

Les cookies ne peuvent normalement être lus que par le serveur Web qui les a émis car ils sont cryptés mais ce n'est pas incassable et il est alors possible de lire des cookies à partir d'un autre domaine.

2.1.3. Les moyens de prévention contre une utilisation abusive

- Les navigateurs permettent une gestion des cookies. Cette possibilité a été imposée par les associations américaines et européennes de défense de la vie privée.
- De nombreux logiciels de gestion de cookies existent.
- Effacer les cookies périodiquement permet de contrecarrer les tentatives de surveillance et de traçabilité des mouvements de l'utilisateur en ligne, la surveillance ne pouvant se faire que sur une courte période. Le profilage devient alors difficile à effectuer.
- Il existe des intermédiaires (logiciel ou service en ligne) qui fonctionnent comme des filtres ou écrans entre l'utilisateur et les sites visités.
- Certains navigateurs permettent de rejeter les cookies ne provenant pas du site que l'on est en train de visiter.

Le seul danger des cookies est pour la vie privée. Il faut bien avoir en mémoire que le cookie ne contient que les informations personnelles que l'on a soi-même indiqué sur un site (mis à part l'adresse IP, le système d'exploitation…). Une des meilleures méthodes de prévention est donc de divulguer le moins d'informations personnelles sur les sites Internet et d'effacer régulièrement les cookies stockés.

2.2 / Les Web bugs ou 1-pixel gifs (pixels invisibles)

Un web bug est une image GIF invisible de petite taille (classiquement 1 pixel) qui permet de surveiller le comportement des internautes en envoyant des informations à un serveur.

C'est un mouchard caché en micro-image invisible dans une page Web ou un e-mail, servant à déclencher l'exécution d'un script depuis un site extérieur.

Sa fonction première est de mesurer l'audience des publicités et de tracer et profiler l'internaute. Le web bug est un tag (pointeur) html (le plus courant étant .img) qui est invisible à l'écran.

Mais ce sont surtout des outils de traçage et aussi de statistiques dont les bénéficiaires sont en général des régies publicitaires ou sociétés de mesures d'audience qui proposent en échange des services à l'administrateur de site. Cela permet de cibler la publicité donc d'avoir plus d'impact et moins d'effet de saturation.

Le problème est qu'on peut associer à ces images une ou deux actions. Le navigateur va les exécuter comme tous les autres scripts. Ainsi on peut récupérer différentes informations comme le type de navigateur, le système d'exploitation, la résolution d'écran, la page visitée avec les mots clés et le cookie du site qui peut contenir des informations personnelles si on a rempli un formulaire.

Le web bug peut aussi être insérer dans un e-mail de manière à savoir combien de personnes vont lire la page.

Les principales utilisations des web bugs (source Privacy Foundation)

- Compter le nombre de fois où une page particulière est consultée,
- Transférer des données telles que le sexe, l'age, le pays… sur les visiteurs d'un site à une société de marketing qui crée ensuite des catégories,
- Transférer des informations personnelles comme le nom, l'adresse, le numéro de téléphone, l'adresse électronique… des visiteurs à une société de marketing. Ces informations peuvent être ensuite croisées avec d'autres informations comme le nombre de personnes dans le foyer, le type de cartes possédées…,
- Lister les pages Web consultées sur différents sites par chaque visiteur,
- Transmettre les recherches effectuées par un visiteur sur un moteur de recherche à une société de marketing. Les recherches effectuées permettent de créer un profile type d'internaute.

- Associer un achat à une bannière publicitaire visualisée par l'internaute avant son achat. De manière générale, le site qui affiche ces bannières touche un pourcentage de la vente.
- Compter le nombre de fois qu'une bannière publicitaire est apparue,
- Déterminer l'efficacité d'une bannière publicitaire en comptant le nombre de visites sur le site de cette publicité à partir du site d'origine,
- Déterminer les intérêts d'une personne pour tel ou tel produit ou service en suivant les pages visitées sur les différents sites,
- Recevoir des informations comme le type et la configuration du navigateur Internet utilisé. Ces informations sont ensuite agrégées pour déterminer quelle sorte de contenu peut être mis sur un site pour être vu par la majorité des visiteurs,
- Autoriser une tierce partie à fournir des logs de connexion à un site Web qui ne dispose pas de cette fonction lui même.

Leur utilité dans les e-mails :

- Vérifier qu'un individu en particulier a ouvert l'e-mail, ou tester si l'adresse e-mail est valide,
- Vérifier que la personne utilise une messagerie qui lit les messages html,
- Compter le nombre de fois où une bannière publicitaire dans une lettre est visionnée,
- Vérifier si les destinataires ont javascript, java, active X qui fonctionnent sur leur logiciel de messagerie. Cela permet de s'assurer que la publicité va être correctement reçue avec les sons, animations ou vidéo,
- Vérifier combien de fois les rapports de presse sont lus par les reporters et si ces rapports sont transférés à des personnes de leur société ou à des gens extérieurs,
- Détecter de potentielles contre-façons de newsletter (violation de droits d'auteur).
- Compter le nombre de fois où une publicité est visionnée dans les messages des groupes de discussion.

Ainsi le Web bug peut être utilisé seul comme mouchard mais peut aussi être utilisé par les spywares logiciels. Comme le cookie, son utilisation peut être détournée à des fins de traçage mais avec deux particularités qui le rende beaucoup plus dangereux : le fait qu'il soit invisible et qu'il puisse effectuer des actions à l'insu de l'internaute.
Les moyens de prévention sont à peu près similaires à ceux des cookies, il n'est donc pas utile de les répéter ici.

2.3 / La Législation

Le premier point est de savoir si les informations enregistrées par les cookies sont considérées comme des données à caractère personnel ou non.
D'après l'article 4 de la loi du 6 janvier 1978 (cité dans l'introduction), les cookies donneraient des informations indirectes : adresse IP, système d'exploitation… sans qu'il y ait eu d'information préalable (droit à l'information préalable).
De même, d'après la directive 95/46/CE (voir dans l'introduction), un numéro d'identification est considéré comme une donnée à caractère personnel.

Un exemple de jurisprudence démontrant une utilisation détournée des cookies est celui de DoubleClick. Cette régie publicitaire a dû abandonner son projet de fichage nominatif des internautes visitant les sites de ses clients. Lorsqu'un utilisateur visitait pour la première fois un site web qui apposait les bandeaux publicitaires de DoubleClick, il lui assignait un Guid qu'il mémorisait dans un cookie sur l'ordinateur de l'internaute. Lorsque que l'internaute revenait sur un de ces sites (environ 13000 !), le cookie était lu et enregistrait dans une base de donnée son Guid auquel était rattaché les noms des sites visitées et les renseignements personnels que l'internaute avait pu saisir sur l'une de ces pages.

C'est la directive 2002/58/CE qui est la plus précise sur le sujet : les points 24 et 25 précisent l'utilisation qui peut être faite des cookies et web bugs.
Le point 24 a été cité en introduction et précise que les cookies et web bugs ne doivent être utilisés qu'à des fins légitimes, c'est à dire en ne portant pas atteinte à la vie privée et en ayant une toute autre utilité que le profilage.

Il semble important de citer ici le point 25, qui bien qu'étant un peu long, prend justement l'exemple des cookies et donne des précisions supplémentaires :

« (25) Cependant, les dispositifs de ce type, par exemple des témoins de connexion (cookies), peuvent constituer un outil légitime et utile, par exemple pour évaluer l'efficacité de la conception d'un site et de la publicité faite pour ce site, ainsi que pour contrôler l'identité des utilisateurs effectuant des transactions en ligne. Lorsque des dispositifs du type précité, tels que des témoins de connexion, sont destinés à des fins légitimes, par exemple faciliter la fourniture de services de la société de l'information, leur utilisation devrait être autorisée à condition que les utilisateurs se voient donner des informations claires et précises, conformément à la directive 95/46/CE, sur la finalité des témoins de connexion ou des dispositifs analogues de manière à être au courant des informations placées sur l'équipement terminal qu'ils utilisent. Les utilisateurs devraient avoir la possibilité de refuser qu'un témoin de connexion ou un dispositif similaire soit placé sur leur équipement terminal. Ce point est particulièrement important pour les cas où des utilisateurs autres que l'utilisateur original ont accès à l'équipement terminal et donc aux données sensibles à caractère privé qui y sont stockées. L'information relative à l'utilisation de plusieurs dispositifs à installer sur l'équipement terminal de l'utilisateur ainsi que le droit de refuser ces dispositifs peuvent être offerts en une seule fois pendant une même connexion, et couvrir aussi l'utilisation future qui pourrait être faite de ces dispositifs durant des connexions subséquentes. Les méthodes retenues pour communiquer des informations, offrir un droit de refus ou solliciter le consentement devraient être les plus conviviales possibles. L'accès au contenu d'un site spécifique peut être, toutefois, subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion ou d'un dispositif analogue, si celui-ci est utilisé à des fins légitimes. »

Cette directive indique que l'usage d'un témoin de connexion est justifié pour certaines utilisations mais que l'utilisateur doit être prévenu de sa fonction et pouvoir le refuser. Le mot « convivial » sous-entend que les moyens mis en oeuvre pour informer l'internaute et lui permettre de les accepter ou non doivent être clairs et simples.

III / Les fichiers LOG

Au niveau d'un serveur, un fichier log est un fichier enregistrant les opérations des utilisateurs, qui contient donc les informations de connexion. Ce sont les logs de connexion.
De manière plus générale c'est un journal des événements s'étant produits sur un système.

C'est le premier aspect de la vie privée : les échanges de mails passent par des ressources publiques.
Ces fichiers peuvent permettre de retracer ce qui a été fait sur un ordinateur ou les recherches effectuées sur Internet : ce sont toutes les données techniques qui servent à identifier le moindre échange d'un utilisateur sur tout type de réseau, véritables profils intimes de correspondances privées. Les FAI peuvent retracer ainsi toutes les activités d'un utilisateur dans le cas d'une enquête.

Ce sont aussi les traces au niveau applicatif dans les entreprises : ils peuvent être un moyen de contrôle de l'activité des salariés.

3.1/ La législation française sur les fichiers log

Les autorités demandent aux FAI de conserver ces fichiers à des fins préventives : décrets portant sur l'article 29 de la LSQ, loi relative à la sécurité quotidienne du 15 novembre 2001. La LSQ ordonne aux prestataires de services (FAI) de conserver les données ou logs de connexion pendant un an :

« II. Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs. »

Cette loi autorise également les juges à recourir aux « moyens de l'État soumis au secret de la Défense nationale » pour décrypter les messages.

Un article défend tout de même la vie privée, le contenu ne devant pas être étudié et le traçage est interdit :

« *IV. Les données conservées et traitées dans les conditions définies aux II et III portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers.*

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.
La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article. »

Par cette loi les fournisseurs d'accès ont l'obligation de garder ces logs durant un an mais certains sont très réticents et n'ont pas encore mis en place ce stockage, le décret d'application n'étant pas encore passé.

« I. Est puni d'un an d'emprisonnement et de 75 000 Euros d'amende le fait pour un opérateur de télécommunications ou ses agents :
1. De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi ;
2. De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi. »
(Art. L. 39-3.)

3.2/ « Les recommandations » du G8 sur les logs de connexion

Les membres du G8 ont mis en place le 13 et 14 mai 2002 une série de «Recommandations sur le dépistage des communications électroniques transfrontalières dans le cadre des enquêtes sur les activités criminelles et terroristes», document en gestation depuis 1999. Il a pour objectif *« d'aider nos organismes de police et de sécurité nationale à localiser et identifier rapidement les criminels et les terroristes qui se servent des réseaux de communication internationaux à des fins illicites»*. Ainsi, le terrorisme international est la raison principale de ces recommandations : c'est une justification de sécurité nationale des différents états, ce qui selon la loi est une des raisons autorisant les États à intercepter des correspondances personnelles (en France loi du 10 juillet 1991, article 3 cité dans la première partie).

Pourtant le 18 juillet 2002, la commission parlementaire des libertés du citoyen a encore une fois appliqué le principe de droit à l'oubli.

Une liste de 10 points a été établie : les points un à six sont spécifiques au protocole Internet et sont issus d'une liste publiée officiellement par un comité d'experts du Groupe du G8, le 15 mai 2002, et les points 7 à 10 émanent de la réunion du 11 avril à la Haye, siège de Europol (office européen de coopération policière) et concernent la téléphonie fixe et mobile.

Dans les points spécifiques aux protocoles Internet, on trouve : les systèmes d'accès au réseau (SAR), les serveurs de courriel, les serveurs de téléchargement en amont et en aval, les serveurs Web, le réseau USENET, le service de bavardage Internet (IRC).
Pour ce qui est de la téléphonie, le point 7 précise tout ce qui se rapporte aux lignes fixes, le point 8 aux lignes mobiles et satellites, puis un point sur les formats de numéros et le temps synchronisé. (La liste dressée par Europol se trouve en annexe 3.)

L’application de la LSQ et de ces recommandations va demander des capacités de stockage immenses.

Des données personnelles pourront être communiquées à des autorités étrangères et ne seront effacées qu’en cas d’acquittement ou de relaxe. La durée des procédures pénales étant souvent très longues, de nombreuses personnes innocentes seront fichés durant plusieurs années.
La fédération informatique et liberté (FIL) a été créé le 9 juillet 2002 face à cette montée de la surveillance. Elle regroupe une vingtaine d’associations dont reporters sans frontière.

IV / Les autres ressources à risque

4.1/ Les VBScripts, la technologie Active X et les CGI

Les scripts sont des suites de lignes de codes, ce ne sont pas réellement des programmes mais ils peuvent faire exécuter certaines actions à un logiciel.

4.1.1. Les scripts CGI (Common Gateway Interphase)

Programmes situés sur le serveur qui peuvent être exécutés à partir des pages HTML. Ils sont souvent utilisés pour accéder à une base de données, ils permettent l'exécution de programmes spécifiques sur un serveur. Chaque connexion provoque le lancement, l'exécution, et la fin d'un programme indépendant généralement écrit en C, C++, Perl ou TCL.

Principal trou de sécurité sur un serveur World Wide Web car si l'installation est faite par défaut lors de l'installation d'un site Web, il y a de grande chance d'installer des scripts CGI présentant des trous de sécurité connus. Ces bugs pourront permettre à des pirates informatiques de récupérer des mots de passe ou d'autres informations.

4.1.2. Les VBScripts

Les scripts Virtual Basic sont des scripts dont le code peut être interprété par des applications Microsoft via ActiveX Scripting ou par des contrôles ActiveX présents dans Windows. L'écriture sur le disque dur et dans le registre de Windows est possible contrairement aux Scripts Java.

Par la consultation d'une page web contenant un script Virtual Basic adéquate on peut effectuer des opérations non autorisées, comme l'écriture, la suppression, la modification d'un fichier sur l'ordinateur. En effet un VBScript contenu sur un page html est interprété par défaut par Internet Explorer. Cette faille a été utilisée par des chevaux de Troie, des programmes permettent de créer des pages web implantant automatiquement un cheval de Troie.

4.1.3. La technologie Active X

Technologie propriétaire de Microsoft, permettant l'incorporation de petits programmes à des documents Internet (HTML), lesquels sont exécutés localement par le navigateur.

Les active X sont dangereux parce qu'ils peuvent accéder sans restriction à toutes les ressources du système hôte (on ne peut pas empêcher un active X d'écrire sur le disque ou d'utiliser les ressources réseaux) : cette technologie permet un contrôle du système sur lequel il s'exécute.

Ils sont très utilisés par les pirates ou par des logiciels espions puisqu'il est possible de programmer facilement des vers ou des chevaux de Troie avec des Active X.

Prévention :

- Vérifier la source de l'active X : présence d'un certificat provenant d'une source sure.
- Désactiver la gestion des Active X ou restreindre les possibilités d'exécution des contenus active X dans les logiciels de navigation et de courrier.
- Ne pas engager d'actions d'auto exécution des scripts et des macros dans les logiciels.

4.2/ Les failles de logiciels et systèmes d'exploitation

Il y a trois types de failles logicielles :

- Des fonctions cachées ou non signalées dans la documentation remise à l'utilisateur mais activables par un tiers. Souvent ces fonctions sont anodines et ne relèvent que de l'amusement du concepteur.

- Elles peuvent être également des programmes espions dans les logiciels de commerce : ce sont des fonctions non détectées que l'on appelle alors backdoor ou portes dérobées puisqu'elles permettent à un tiers d'accéder à un ordinateur (cheval de Troie).

- Les bugs ou trou de sécurité fréquemment trouvés dans Internet Explorer ou Windows, qui sont des erreurs de conception engendrant des problèmes plus ou moins importants de sécurité.

Dans tous les cas, ces failles permettent à des tiers de consulter des informations personnelles ou confidentielles. Le Cert d'Intexxia estime que 60% des failles proviennent de lacunes dans les développements. La question de la faille volontaire ou non s'est posée, mais aucune preuve n'a été trouvée, mis à part la découverte de Andrew Fernandes qui identifia dans Windows une ligne de code faisant référence à la NSA. Il semble pourtant que certaines ont été créées sciemment, la question est alors plus de savoir à quelles fins, commerciales ou d'espionnage.

Les utilisateurs ne sont pas assez sensibilisés aux risques qu'elles entraînent et ils oublient souvent d'installer les nouveaux correctifs. Mais les alertes permanentes tuent l'information : elles sont trop nombreuses et les utilisateurs ne prennent pas le temps de s'informer.

Une question se pose à ce sujet : faut-il avertir tous les internautes lorsque l'on découvre une faille de sécurité ? Le risque est que d'autres personnes ne l'ayant pas découverte s'en servent avant que le correctif ne soit disponible. Or certains internautes croient bon de propager des informations sur des vulnérabilités plutôt que de prévenir d'abord l'éditeur. Cela s'ajoute au nombre des alertes suffisamment important et créé un danger encore plus grand.

4.3/ Les réseaux sans fil (WLAN)

L'émergence des réseaux sans fils, ou Wireless Local Area Network, pose des problèmes de sécurité, car les technologies de sécurité s'y référents ne sont pas encore au point et parce que le public n'est pas encore assez sensibilisé aux problèmes de sécurité liés qu'elles entraînent.

- **Les risques des procédés utilisant la transmission radio sont de plusieurs ordres :**

  - Les communications peuvent être captées ou écoutées : avec un ordinateur portable équipé d'une carte 802.11 (Wi-fi) on peut capter certains réseaux de grandes entreprises !
  - Elles permettent une usurpation d'accès sur l'ordinateur et d'avoir accès à toutes les données résidant sur le disque dur.
  - Elles peuvent être brouillées car la ressource des fréquences radio est partagée donc saturable.
  - Facilité et faible coût de mise en œuvre : des réseaux pirates sont très simple à mettre en oeuvre. Avec un peu de connaissances techniques sur le branchement des câbles, il est facile de raccorder un réseau sans fil (WLAN) au réseau LAN (Local Area Network).
  - Connexion accidentelle : les portables qui ont cette ressource, si celle-ci n'est pas désactivée, risque de se connecter par erreur à un réseau sans fil. C'est ce qui s'est passé à Londres lorsque le RSA a mis en place des « pot de miel » (leurre) pour tester la sécurité de ces réseaux. 75% des personnes qui se sont connectées sur ce leurre l'ont fait par accident et sans le savoir. Cela serait du à Windows XP qui détecte automatiquement les réseaux sans fil avoisinants et s'y connecte par défaut.

- **La technologie sans fil Wi-fi** (Wireless Fidelity) correspond aux normes de communication radioélectrique 802.11. La 802.11b repose sur des fréquences (2,4 GHz) qui étaient à l'origine réservées à l'armée.

Si ce genre de réseau n'est pas protégé, il suffit simplement d'un ordinateur portable, qui peut espionner le réseau à distance ou un accès internet. En effet, le Wi-fi tel quel, n'a pas de barrière de sécurité, il faut absolument utiliser un logiciel de chiffrement. Le problème actuel est que beaucoup de gens l'oublient encore ou ne sont pas assez sensibilisés sur ce point. De plus les normes de fonctionnement des réseaux Wi-fi n'intègrent pas les mesures de cryptage qui seraient nécessaires. Les normes 802.11a et b présentent de sérieuses lacunes en matière de sécurité et donc de confidentialité. C'est pour cela que de nouvelles normes dont la 802.11i sont en cours d'élaboration, normes qui intégreraient des procédés de cryptage et d'authentification plus robustes.

- **Mesures préventives :**

  - ne pas laisser les ordinateurs personnels allumés et connectés en permanence au réseau local radio.
  - Mettre en place une liste de contrôle d'accès énumérant les adresses physiques des cartes Wi-fi utilisées (@mac).

- Système de pare feu entre le réseau sans fil et le réseau local préexistant.
- Une architecture VPN (Virtual Private Network) convient encore mieux : en effet un réseau privée virtuel est déjà une protection importante puisque ce sont des canaux sécurisés.
- Sensibilisation des utilisateurs aux risques potentiels des réseaux sans fil.

Dans les entreprises une politique concernant le sans fil doit être définie (pour les plates-formes et les périphériques) comprenant une politique utilisateur.

- **Le cadre légal :**

Le Wi-fi en France n'est pas encore d'un usage libre en espace public ou en plein air. Le législateur autorise les fournisseurs de services à installer des bornes d'accès (AP) 2,4 GHz sous certaines conditions et dans certains départements.
Les opérateurs voulant offrir des services au public doivent demander une autorisation, gratuite et temporaire. Les demandes sont soumises à l'approbation du ministère de la Défense afin de ne pas perturber les réseaux militaires.

V / Les Contre-mesures

Nous parlerons ici de mesure de prévention et des contre-mesures et techniques d'anonymat liés aux mouchards et dérivés. On ne rentrera donc pas dans tous ce qui est anonymat de messagerie, cryptographie et stéganographie, bien que ces dernières puissent bien sûr permettre de protéger des informations personnelles qui ne pourraient alors pas être lues si elles étaient récupérées par un mouchard.

5.1 / Le firewall (pare feu) : protecteur ou espion ?

Protection logicielle ou matérielle qui a pour mission de protéger les échanges de données entre une machine et le réseau internet. Il analyse les paquets IP qui circulent afin de filtrer le flux de données entrant et sortant.

- Protection contre les intrusions : il permet de fermer les ports non utilisés (en particulier sous Windows les ports 137 à 139 qui sont très dangereux) et contrôle les applets java et Active X.

- Surveillance des informations sortantes : on peut contrôler les informations émises par les spywares si on en a, ou bien justement les déceler grâce au firewall et les bloquer. De la même manière on peut déceler l'existence d'un cheval de troie. En effet dans ces différents cas on aura des sorties d'informations automatiques non autorisées.

Mais il permet aussi dans une entreprise de voir tout ce qui est fait sur Internet car il détient toutes les traces de l'activité qui transite par lui : il devient alors plus ou moins un mouchard vis-à-vis des salariés de l'entreprise (navigation sur Internet mais aussi tous les messages entrants et sortants et les pièces jointes).

Le pare feu est à la fois un outil de sécurité mais peut aussi être un outil de surveillance de l'activité des salariés sur Internet.

5.2 / Les techniques d'anonymat et les proxies

Un proxy est un serveur recevant des requêtes qui ne lui sont pas destinées et les transmet aux autres serveurs. Un proxy a deux utilités principales : permet d'avoir accès à des ressources sans prendre de risques lorsqu'on est derrière un firewall et comme le proxy stocke le résultat lorsqu'il reçoit une requête, il fonctionne alors comme un cache. Un proxy peut être intercalé un peu partout pour ajouter une extension à un serveur.

Tout d'abord il n'y a pas d'anonymat total possible sur Internet, on peut toujours retrouver l'origine, mais cette recherche peut être rendue plus difficile et déjouer les systèmes automatiques comme les cookies…

Les serveurs proxies proposent ce type d'anonymat : les différents sites visités n'auront plus accès à l'adresse ip de l'internaute ni aux différentes caractéristiques transmissent en temps normal. Mais le proxy connaît la véritable adresse, il est donc toujours possible de remonter la trace.

Il y a différentes techniques :

- soit aller sur le site et taper directement l'adresse du site auquel on désire accéder,
- soit insérer une ligne de commande dans le navigateur et il n'y a plus besoin d'aller sur le site pour accéder au service d'anonymat,
- soit utiliser des applications qui fonctionnent en tâche de fond et qui offrent une liste de serveurs proxies,
- soit enfin se servir de solutions mixtes : logiciel plus proxy Web. Elles donnent un niveau de sécurité plus élevé mais sont souvent payantes.

Il existe également différentes sortes de proxies :

- Les proxies totalement anonymes qui masquent l'adresse IP et le fait que l'on passe par un proxy.
- Les proxies anonymes de sous classes : l'adresse IP est conservée mais sous une autre forme dans la requête qu'il fait au serveur, l'anonymat n'est pas toujours garanti.
- Les proxies qui en plus de l'IP, changent toutes les autres données (système d'exploitation, navigateur…) mais sont détectables et beaucoup d'administrateur de serveurs refusent les requêtes provenant de ces proxies.
- Les proxies transparents qui ne servent qu'à augmenter la rapidité.

Les FAI stockent les pages que l'on visite et disposent donc d'énormément d'informations sur leurs clients. Pour éviter cela on peut configurer un accès direct à Internet, sans passer par le proxy du FAI. Cela va rendre la connexion un peu plus lente pour les pages les plus populaires, qui sont en général présentes dans les proxy des fournisseurs d'accès, mais rend plus rapide l'accès aux autres sites (évite la requête pour vérifier si la page est présente dans le proxy ou non).

Une autre technique est de créer un tunnel (liaison cryptée entre l'ordinateur et le service utilisé comme proxy). Les données envoyées au proxy sont cryptés et le FAI ne peut pas les lire. Ces proxies sont en général payants.

En revanche, les proxies utilisés par les entreprises pour augmenter la rapidité peuvent être une source d'information sur l'activité des salariés. Mais pour cela il faut que le proxy soit interne à l'entreprise.

5.3/ Projet l'« informatique de confiance » (trusted computing) et NGSCB (Palladium).

Ce sont des technologies qui permettent à une tierce personne de contrôler l'utilisation des contenus disponibles sur l'ordinateur, au sens de limitation de l'utilisation et non pas de surveillance (bien que ce soit possible).

Comme on l'a vu tout au long de ce mémoire, le système d'exploitation le plus exposé à ces différents types de mouchards et aux problèmes de sécurité est Windows : tout d'abord car c'est le plus utilisé au niveau du grand public et qu'il contient en plus de nombreuses failles facilement exploitables, souvent dues à des technologies assez dangereuses qui lui sont propres (comme les active X). De plus, les logiciels de navigation et de messagerie utilisés sont les plus attaqués, toujours grâce à l'utilisation de failles (les chevaux de Troie s'en servent énormément…). De plus les mouchards touchent dans ce cas un plus grand nombre de personnes qui ont un système de protection bien moins développé qu'une grande entreprise.

Face à ce constat et aux récriminations importantes faites à Microsoft celui-ci à mis en place un projet ayant comme but la sécurisation des ordinateurs.

5.3.1. Le Trust Computing Group et TCPA

TCPA, Trust Computing Platform Alliance ou alliance pour une informatique de confiance, est un consortium qui regroupait à l'origine Compaq, HP, IBM, Intel et Microsoft depuis 1999. AMD avait été rajouté et Compaq a été racheté par HP.

Le consortium TCPA a changé de nom et de raison social le 8 avril 2003 et s'appelle aujourd'hui le Trust Computing Group (TCG) qui regroupe AMD, Intel Corporation, IBM, HP, Microsoft : il reprend les spécifications du TCPA, et propose également la création de logiciels correspondants. Il a pour but de définir des spécifications pour une informatique plus sûre, "de confiance" et a défini comme objectif « d'améliorer la confiance et la sécurité sur les plates-formes et systèmes informatiques »

Le projet du TCG est composé de deux choses : le TPM (Trusted Platform Module), c'est à dire une famille de matériels appelé puce Fritz et un logiciel qui permet de le paramétrer.

Les premières puces sont externes au processeur (IBM) : une puce Fritz, puce de type carte à puce ou un périphérique dongle, est soudée à la carte mère pour les premières versions. Il n'y a pour l'instant qu'IBM qui commercialise une puce correspondant aux spécifications TCPA. Ainsi Atmel vend une puce Fritz dans les portables IBM type Thinkpad et les ordinateurs de bureau les netvista depuis mars 2002.
Adrian Horne, directeur marketing Europe de la division PC d'IBM, en explique le rôle : "Cette puce de sécurité garantit plutôt la sécurité locale du système, mais fournit aussi un certain niveau de sécurité pour les accès réseau." Elle permet notamment de verrouiller les informations personnelles sensibles de l'utilisateur.

A partir de la phase 2, cette puce sera dotée d'un identifiant unique et sera intégrée au niveau de la carte mère (bus LPC), cette phase est prévue pour 2005 et c'est alors Intel qui proposera une puce de chiffrement à la norme TCG, projet appelée « LaGrande ».

Cette technologie est également prévue pour être incorporée dans les téléphones mobiles et les PDA.

Principe :

L'ordinateur inclut un procédé de chiffrement et de signature, dont les clés ne sont pas connues de l'utilisateur. En effet cette puce comporte une mémoire permettant de stocker les

clés de chiffrement des données protégées, chiffrement assuré grâce à l'algorithme AES (successeur du puissant DES), à clé symétrique (une seule clé secrète pour chiffrer et déchiffrer), dont la taille de clé va jusqu'à 256 bits.

Au démarrage, la puce vérifie que la ROM est conforme, puis une partie du système d'exploitation. Le périmètre de confiance est constitué du matériel et des logiciels connus et vérifiés et peut donc être étendus régulièrement grâce à une table du matériel et des logiciels dont l'OS tenue à jour.
La puce va vérifier que les composants matériels sont sur la liste approuvée TCG et que les composants logiciels n'ont pas un numéro de série résilié et qu'ils sont bien signés.
Si des modifications dans la configuration du pc ont été effectuées, l'ordinateur va devoir être reconnecté pour être certifié en ligne.
Ensuite c'est un logiciel de surveillance du système d'exploitation qui prend le relais.

5.3.2. Le NGSCB ou Palladium

NGSCB, Next Generation Secure Computing Base ou plate-forme informatique sécurisée de nouvelle génération (depuis le 24 janvier 2003), anciennement Palladium (projet commencé en 1997), est une technologie logiciel de Microsoft. Microsoft a du modifier son nom car une autre entreprise l'utilisait déjà en tant que marque mais a gardé le nom de code Palladium en interne. Le NGSCB est un environnement applicatif pour la gestion des composants TCG que Microsoft intégrera à Windows Longhorn, le successeur de Windows XP, prévu pour 2005. C'est un module ajouté au noyau de Windows.

Le NGSCB sera composé de trois modules :
- un système d'authentification du code et des communications
- un système de cryptage des données
- un système de contrôle des accès et des droits numériques.

Ces trois modules formeront un système tournant en parallèle de Windows et ne se chargeront que de la sécurité et de la stabilité du système.

La partie matériel, une puce répondant aux spécifications TCPA, est appelée SSC (Security Support Component). Elle fournit la clé racine principale.

Le Nexus, partie du système d'exploitation, interagit avec le SSC inclus dans le matériel.
Pour chaque exécution ou consultation d'un document le système d'exploitation vérifiera à distance sur un serveur centralisé la légitimité de cette action et accordera ou non le certificat pour réaliser l'opération. L'identifiant unique du SSC fournira les informations nécessaires aux agents de confiance pour permettre à ceux-ci de gérer les autorisations nécessaires pour tel ou tel fichier.

Pour l'accès à un fichier, l'ordinateur devra alors contrôler plusieurs points essentiels à la sécurité :
- la conformité du logiciel (est-ce un agent de confiance ?)
- la conformité des périphériques (est ce que ce sont les périphériques autorisés aux transactions ?)
- la conformité de droits d'accès (droits d'auteur, certificats de confidentialité…)

Les applications interagissent avec le Nexus de façon sécurisée, ce qui permet de stocker les documents confidentiels dans une « chambre forte » (zone de stockage sécurisée).

5.3.3.Les buts de ces projets

- **Mesure contre la fraude** :

- Cette puce est prévue pour la gestion des droits numériques (DRM : Digital Right Management), c'est à dire le contrôle de contenus protégés par copyright.
(DRMP : Digital Right Management Password)

Ainsi le peer to peer deviendra impossible. En effet le système vérifiera à chaque écoute d'un fichier mp3 que le digital password est bien valide.
Mais il semble que le DRM sera totalement indépendant du NGSCB : la DRM ne sera pas activée par défaut. Ainsi le NGSCB pourra fonctionner sans la technologie DRM et la technologie DRM pourra être installée sur des ordinateurs n'ayant pas le NGSCB.

- De même pour les logiciels, le système vérifie la validité de la licence : le principe est qu'une utilisation non autorisée d'un logiciel entraînera la désactivation de celui ci lors du chargement.

Le système prévoit également l'élimination des contenus piratés : ainsi une liste noire des mauvais fichiers sera téléchargée et des fichiers pourront être radiés en fonction du contenu, du numéro de série de l'application qui les a créés ou d'autres critères. Il prévoit aussi une liste noire mondiale des numéros de série de toutes les copies d'office qui ont été piratées.

- **Une meilleure sécurité :**

- Pour les paiements sécurisés, le commerce électronique souffrant d'un manque de confiance.
- Sécurité logicielle : une meilleure protection contre les virus.
- Renforcement de la confidentialité des données personnelles et sensibles et les sécurisations matérielles et logicielles ne permettront plus l'usurpation d'identité.

- **Autres utilisations possibles :**

- Mise en place de conditions d'accès plus restrictives sur des documents confidentiels : c'est à dire que certains types de fichiers ne pourront être lus que sur des ordinateurs ayant les même autorisations. C'est le contrôle d'accès obligatoire (mandatory acces control). C'est très utile pour les gouvernements. Ainsi on pourra configurer un traitement de texte pour que les fichiers créés ne puissent être lus que par un groupe défini, ou par une entreprise. De la même manière, cette technologie interdira l'accès aux formats des fichiers des logiciels. Ainsi si on envoie un fichier, il ne pourra être lu que par un ordinateur ayant cette technologie.
- Possibilité de créer des dates de péremption sur les fichiers.
- Rendra possible la location de logiciel.
- Certains services de sites Web ne pourront être accessibles qu'aux ordinateurs possédant cette technologie.

Mais avec le projet palladium l'utilisateur n'a plus le contrôle de son ordinateur, c'est l'éditeur qui contrôle l'utilisateur.
Un virus rend le système inaccessible car il va considérer que les licences sont illégales… Il devient alors impossible de réinstaller.
De plus si quelqu'un accède aux autorisations des personnes habilitées il peut alors faire tous ce qu'il veut dans un nombre incalculable d'ordinateurs. Toute attaque du système du registre de mots de passe, d'espionnage, infectera tous les ordinateurs reliés au système.

5.3.4. Les risques économiques

- Avec ce système il n'est plus possible d'effectuer des modifications sur un logiciel, autrement il n'est plus autorisé.
  De plus toute création de nouveau logiciel demandera d'avoir une certification par une autorité compétente pour que le système le reconnaisse et qu'il puisse fonctionner. Or il est assez difficile d'obtenir des certifications dans le cas des logiciels libres étant donné qu'ils peuvent être modifiés et compilés sur chaque machine et que les certifications coûtent chères. Ce projet réduirait alors énormément le nombre de logiciels libres et de ce fait, la concurrence.

- Un autre problème qui n'a pas encore été résolu, est que les fichiers créés par un logiciel NGSCB ne pourront être lus que par un ordinateur ayant ce système. Il y a donc là un autre problème important de limitation de la concurrence que Microsoft doit régler.
- De plus ce système risque de faire disparaître toute l'industrie des antivirus, des firewalls, les systèmes de destruction d'intrusion…

- La puce Fritz va évincer les cartes à puce du marché de l'identification et ce sont les pays européens qui vont être les premiers touchés (l'industrie européenne de la carte à puce est très puissante).

- Enfin, si on veut que ce nouveau système soit efficace, en plus du coût de son installation, il faudra également renouveler tout le parc informatique que ce soit au niveau matériel ou logiciel. En effet il ne prendra toute son envergure qu'avec les nouveaux matériels et logiciels développés pour cette technologie.

5.3.5. La possibilité de désactivation

Face à la levée de bouclier qu'a entraînée l'annonce du projet Palladium, les défendeurs de ce système ont précisé qu'il serait possible de désactiver le système ou de réduire ses effets. Le problème est que dans ce cas tous les logiciels liés à cette technologie ne fonctionneraient plus ou fonctionneraient très mal. Il faudra alors utiliser les logiciels non sécurisés.
De plus pour certains services sur Internet, on pourrait ne pas y accéder si le système est désactivé.
Une fois désactivé on retrouvera peut être un peu de la liberté que l'on avait avant mais on aura beaucoup moins de choix au niveau des logiciels. Microsoft a déclaré que le NGSCB permettrait de faire cohabiter des logiciels de confiance et les autres, ce qui n'est pas le cas de TCPA seul.

Le NGSCB sera désactivé par défaut, l'utilisateur pourra choisir d'activer ou non les fonctionnalités du NGSCB logicielles ou matérielles.
Mais par contre si un utilisateur désactive un système, il ne pourra plus être réactivé. Voilà qui risque de limiter de beaucoup les désactivations…

En revanche, la puce, même avec le système désactivé, n'ignorera pas les logiciels piratés.
L'effet de la désactivation est que l'ordinateur ne démarre plus en mode de confiance, mais il vérifie toujours le système d'exploitation. La désactivation ne sera donc jamais totale.
Ce projet, utilisé différemment, peut devenir un énorme mouchard, le meilleur jamais conçu. Si ce projet aboutit, cela signifie que tous les ordinateurs avec ce système seront contrôlés de l'extérieur et référencés. L'ordinateur ne sera plus du domaine privé…

5.3.6. Au niveau du droit

La première question venant à l'esprit est pourquoi les lois sur la protection de la vie privée et sur la concurrence déloyale ne rendent pas ce projet caduque. Cela vient du DMCA (Digital Millenium Copyright Act). En Europe c'est l'EUCD (European Union Copyright Directive), qui a été transposée en France le 4 avril 2003 dans un avant-projet de loi portant le même nom.

Ces Lois obligent les fabricants de matériels et de logiciels à ne fournir que des produits empêchant le piratage. Ainsi, par exemple, un graveur ne devrait pas pouvoir graver de cd ne possédant pas de copyright et les lecteurs multimédia ne devraient pas pouvoir lire les mp3 piratés. Donc le DMCA interdit de casser la puce Fritz.
Le projet Palladium / TCPA remplit exactement les conditions demandées par ces lois.

Ce projet montre une fois de plus que la limite entre la protection contre la fraude, la sécurité et la protection de la vie privée est très floue. Ces projets signifient que l'utilisateur n'aura plus le choix : que ce soit au niveau matériel ou logiciel. De plus la différenciation entre les deux projets est très floue. Beaucoup les confondent, et rien n'est fait, que ce soit par le consortium TGC ou par Microsoft, pour éclaircir la situation. De plus le projet Palladium est modifié au fur et à mesure et les communiqués de Microsoft change de ton tous les six mois. Il est donc encore assez difficile de voir réellement les dangers liés à ce projet et de vérifier leur validité.

Conclusion

Le modèle économique du net repose sur la publicité et le « profiling ». Internet semble gratuit mais en réalité chacun se rémunère par des moyens différents : les publicités ciblées, les spywares, l'étude de profil revendu ensuite…
Si tous ces moyens permettant ce genre de rémunération étaient totalement bloqués ou interdits (chose plus ou moins impossible en raison de la vitesse à laquelle naissent de nouvelles technologies et de l'impossibilité d'être totalement anonyme sur le net) ou n'existait pas, est ce qu'Internet tel qu'on le connaît existerait ?

Oui. Car le « profiling » n'est pas l'unique rémunération de ces entreprises et Internet est un très bon moyen de se faire connaître et d'élargir son champ d'action. En revanche de nombreux sites n'ont pas un but pécuniaire, mais cherchent à partager des connaissances ou des passions (sites personnels, associations…) : Internet est avant tout un moyen d'expression et d'ouverture au monde et à la connaissance.

Malheureusement aujourd'hui encore, de nombreux pays restreignent l'accès à Internet, que ce soit par manque d'infrastructures ou par la censure de l'information. Les traces servent, dans ces pays, à limiter l'accès à de nombreux sites. Mais des tentatives sont faites aussi dans les pays où la vie privée et la liberté d'expression sont censées être acquises : le gouvernement américain a tenté de poser des filtres sur les ordinateurs des bibliothèques publiques…

Face aux dangers grandissant du net, les internautes sont de plus en plus à la recherche de sécurité, alors même que la plupart sont très loin d'être informés des risques potentiels.

Les différents projets répondent à cette attente :

- La sécurité d'État, la sûreté nationale, justifie des projets comme Échelon, Carnivore et d'autres, en particulier depuis le 11 septembre 2001.
- La protection des internautes justifie la naissance de projet comme Palladium et TCPA.
- Les mesures de sécurité dans les entreprises pour éviter les intrusions et protéger les données justifient les outils conservant des traces directement ou indirectement nominatives sur les salariés.
- Les technologies développées contre la fraude justifient les atteintes à la vie privée.
- Les lois de lutte contre la criminalité informatique, donc pour réduire les dangers du net, justifient de contourner les lois de protection de la vie privée.

La sécurité est devenue une justification aux atteintes à la vie privée : la protection des données est un danger pour la vie privée ! En réponse, de nombreuses associations de défense de la vie privée se créent et prennent de l'importance.

On est face à un dilemme : les internautes demandent plus de sécurité pour protéger leurs données personnelles, mais peut-on traiter la sécurité autrement que par le contrôle ? Tous les mécanismes de sécurité sont plus ou moins illégaux car on regarde le contenu.
L'exemple type est le projet Palladium : projet à but totalement sécuritaire et en même tant gigantesque mouchard.

Un recueil de directives pratiques sur la protection des données des travailleurs du 7 octobre 1996 précise que « *les données personnelles collectées en relation avec la mise en œuvre de mesures techniques ou d'organisation visant à garantir la sécurité et le bon fonctionnement des systèmes d'information automatisés ne devraient pas servir à contrôler le comportement des travailleurs* ». Ainsi une surveillance permanente ne peut être autorisée que pour des raisons de santé et de sécurité et en vue de protéger les biens de l'entreprise. Les traitements automatisés sont en général autorisés, tant qu'il n'y a pas intervention humaine. Mais le jour où un problème apparaît, l'intervention humaine est obligatoire. Le principe est le même pour les interceptions de communication.

Les politiques de protection des données doivent viser un juste équilibre entre le respect de la vie privée, la sécurité des réseaux pour les entreprises, la prévention de la fraude, et la lutte contre les activités criminelles et terroristes. Mais il faut également protéger le public si on veut que la confiance envers le commerce électronique grandisse, et qu'Internet reste cette exceptionnelle possibilité d'échange et de liberté.

Annexe 1 : les articles du Code Pénal relatifs à la vie privée

Art. 226-15 (de l'atteinte au secret des correspondances)

(Ordonnance n°2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. »

Article 226-16 (Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques)

(Loi nº 92-1336 du 16 décembre 1992 art. 360 et 373 Journal Officiel du 23 décembre 1992 en vigueur le 1er mars 1994)

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de trois ans d'emprisonnement et de 45000 euros d'amende. »

Art.432-9 (des atteintes au secret des correspondances)

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau de télécommunications autorisé en vertu de l'article L. 33-1 du code des postes et télécommunications ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu. »

Annexe 2 : résumé de la législation européenne sur la vie privée

Définition d'une directive :

Une directive est un acte législatif européen dont les Etats membres sont destinataires. Une fois cette législation adoptée au niveau européen, chaque Etat membre doit en assurer la transposition efficace dans son système juridique. La directive prescrit un résultat final. La forme et les méthodes d'application sont laissées à l'appréciation de chaque Etat membre. En principe, une directive prend effet moyennant des mesures nationales d'application (législation nationale).

Toutefois, il est possible que même lorsqu'un État membre n'a pas encore appliqué une directive, certaines des dispositions de celle ci puissent avoir un effet direct. Ceci signifie que si une directive confère des droits directs aux personnes, des personnes peuvent arguer de la directive devant un juge sans avoir à attendre la transposition de cette directive dans la législation nationale. De surcroît, si les personnes estiment avoir subi un préjudice du fait que les autorités nationales n'ont pas transposé la directive correctement, elles peuvent être habilitées à engager des poursuites en dommages-intérêts. CEs dommages ne peuvent être obtenus qu'auprès des tribunaux nationaux.

Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950

Convention du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement des données à caractères personnels.

Loi du 8 septembre 1992 relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

La Directive 95/46/CE :

Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, du 24 octobre 1995.

Elle a été mise au point pour harmoniser les dispositions nationales dans ce domaine afin de lever tout obstacle à la libre circulation des données à caractère personnel à l'intérieur de l'Union Européenne.

Elle invite les Etats membres à assurer « la protection des droits et libertés fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données »

Le traitement de données à caractère personnel ne peut être effectué qu'avec le consentement de la personne concernée ou s'*« il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées* ».

Les exceptions portent sur la sûreté de l'Etat, la sécurité publique, la défense…

Les Etats de L'UE étaient tenus d'aligner leur législation nationale sur les dispositions de la directive d'ici au 24 octobre 1998. Mais la France n'a adopté un projet de loi en première lecture que le 30 janvier 2002.

La Directive 97/66/CE : directive abrogée par la directive 2002/58/CE

Directive relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

« Les Etats membres garantissent au moyen de réglementations nationales la confidentialité des communications (...). En particulier ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées. »

Avis de la Commission pour la protection de la vie privée relatif au commerce électronique, 22 novembre 2000.

Amendement Européen du 13 novembre 2001 :

Interdisant l'utilisation des réseaux de communications électroniques pour stocker des informations ou pour obtenir un accès à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur sans le consentement préalable explicite de l'abonné ou de l'utilisateur concerné.
La CNIL a fait un communiqué de presse sur cet amendement le 7 décembre 2001.

La Directive 2002/58/CE : directive vie privée et communications électroniques

Directive relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques, du 12 juillet 2002.

Elle abroge la directive 97/66/CE.

Annexe 3 : la liste des log dressés par Europol

1. **Système d'accès au réseau (SAR)**
   - Journaux d'accès particuliers aux serveurs d'authentification et d'autorisation comme TACAS+ ou RADIUS (Remote Authentification Dial-in User Service) utilisés pour contrôler l'accès aux routeurs IP ou aux serveurs d'accès au réseau.
   - date et heure de connexion du client au serveur
   - ID utilisateur
   - adresse IP assignée
   - adresse IP du SAR
   - nombre d'octets transmis et reçus
   - identification de la ligne appelante (ILA).

2. **Serveur de courriel**
   - Journal SMTP (protocole de transfert de courrier simple)
   - date et heure de connexion du client au serveur
   - adresse IP de l'ordinateur d'envoi
   - message-ID (msgid)
   - expéditeur (login@domain)
   - destinataire (login@domain)
   - indicateur de situation
   - journal du POP (Post Office Protocol) ou du IMAP (Protocole d'accès message Internet)
   - date et heure de connexion du client au serveur
   - adresse IP du client connecté au serveur
   - ID utilisateur
   - dans certains cas, renseignements sur le courriel récupéré.

3. **Serveurs de téléchargement en amont et en aval**
   - Journal FTP (protocole de transfert de fichier)
   - date et heure de connexion du client au serveur
   - adresse IP de la source
   - ID utilisateur
   - chemin et nom de fichier des données téléchargées vers l'amont ou l'aval.

4. **Serveurs web**
   - Journal HTTP (protocole de transfert hypertexte)
   - date et heure de connexion du client au serveur
   - adresse IP de la source
   - transaction (c'est-à-dire commande GET)
   - chemin de la transaction (pour récupérer la page html ou l'image)
   - dernière page visitée
   - codes de réponse.

4. **Réseau USENET**
   - Journal NNTP (Network News Transfer Protocol)
   - date et heure de connexion du client au serveur
   - ID du processus (nnrpd[NNN...N])
   - nom d'hôte (nom du serveur de nom de domaine (DNS) de l'adresse dynamique IP assignée)

- activité de base du client (sans contenu)
- message-ID du message livré.

6. **Service de bavardage internet**
   - Journal IRC
   - date et heure de connexion du client au serveur
   - durée de la séance
   - surnom utilisé pendant la connexion IRC
   - nom d'hôte ou adresse IP, ou les deux.

7. **Données devant être conservées par les compagnies de téléphone pour les abonnés de lignes fixes**

A. Liste minimum :
- numéro appelé même si l'appel n'aboutit pas
- numéro appelant même si l'appel n'aboutit pas
- date et heure du début et de la fin de la communication
- type de communication (entrant, sortant, liens vers des services, appels conférence)
- dans le cas d'appels conférence ou de liens vers des services, tous les numéros intermédiaires
- infos à la fois sur l'abonné et sur l'usager (nom, date de naissance, adresse)
- adresse où est envoyée la facture
- dates de début et de résiliation de l'abonnement
- type de communication que l'usager utilise (normal, RNIS, ADSL, et s'il s'agit d'une com à double voie ou pour recevoir seulement)
- numéro appelé ? (Forwarded called number)
- la durée de l'appel
- numéro de compte bancaire / autres modes de paiement.

B. Liste optionnelle:
- copie du contrat
- pour améliorer les méthodes d'investigation, les compagnies de téléphone ["Telcos" dans le texte] devraient être capables de distinguer la nature de la télécommunication: voix/données/fax.

8. Données devant être conservées par les compagnies de téléphone pour les abonnés de lignes mobiles / satellites

A. Liste minimum:
- numéro appelé même si l'appel n'aboutit pas
- numéro appelant même si l'appel n'aboutit pas
- date et heure du début et de la fin de la communication
- type de communication (entrant, sortant, liens vers des services, appels conférence)
- dans le cas d'appels conférence ou d'appels vers des services, tous les numéros intermédiaires
- infos à la fois sur l'abonné et sur l'usager (nom, date de naissance, adresse)
- numéros IMSI et IMEI [identifiant les combinés mobiles]
- adresse où est envoyée la facture
- dates de début et de résiliation de l'abonnement
- identification de l'appareil utilisé par le destinataire de l'appel

- identification et lieu géographique des cellules [hertziennes] utilisées pour relier le destinataire (appelé et usager appelé) sur le réseau de télécommunications
- coordonnées géographiques de l'emplacement de la station au sol du réseau mobile
- service WAP
- service SMS (date et heure des messages entrants et sortants, numéro composé)
- service GPRS
- dans le cas d'appels conférences ou de liens vers des services, tous les numéros intermédiaires
- numéro appelé (Forwarded called number)
- durée de l'appel
- numéro de compte bancaire / autres moyens de paiement
- Les réseaux GPRS et UMTS étant basé sur [le protocole], par conséquent toutes les données mentionnées ci-dessus (comme les adresses IP) devraient être conservées.

B Liste optionnelle:
- copie du contrat
- pour améliorer les méthodes d'investigation, les compagnies de téléphone ["Telcos" dans le texte] devraient être capables de distinguer la nature de la télécommunication: voix/données/fax.

9. Format des numéros

Tous les numéros de téléphone (à la fois pour les ISP et les compagnies de téléphone) devraient être décrits par:
- code pays
- code local [area number]
- numéro d'abonné.

Toutes les informations en code ASCII avec des séparateurs de tabulation et les retours de transport [carriage return]
- certains services pouvant permettre aux usagers de se connecter à l'ISP via des numéros gratuits. Par conséquent, la structure de ce numéro est demandée.

10.Temps synchronisé

Les opérateurs de télécommunications, les fournisseurs d'accès Internet et les fournisseurs de services Internet doivent synchroniser leurs serveurs avec l'heure de leur pays [de résidence] dotée de spécifications GMT.

BIBLIOGRAPHIE

Presse spécialisée

Presse écrite :

http://www.01net.com : site de 01 informatique
http://www.weblmi.com/ : site du monde informatique
http://www.reseaux-telecoms.net : site de Réseaux et Télécoms
http://www.miscmag.com/: Multi-System & Internet Security Cookbook
http://www.zataz.com/ : Hackers & Pirate Magazine

Uniquement en ligne :

http://www.vnunet.com et http://www.vnunet.fr
http://zdnet.fr
http://solutions.journaldunet.com/
http://news.com.com
http://lambda.eu.org/ : bulletin
http://www.transfert.net/
http://www.uzine.net
http://www.cnrs.fr/Infosecu/Revue.html : la revue de la sécurité des systèmes d'information au CRNS (Centre National de la Recherche Scientifique)
http://www.strategic-road.com
http://www.securent-2000.com
http://www.bugbrother.com/
http://www.theregister.co.uk/

Sites de sécurité informatique

En langue française :

http://anonymat.org : les dossiers pratiques. Site qui dénonce les atteintes à la vie privée liées aux nouvelles technologies de l'information et des télécommunications principalement l'informatique et la téléphonie mobile.
http://www.securiteinfo.com
http://www.secuser.com/
http://www.securite.org
http://securis.info/
http://www.echu.org/ : « toute la sécurité informatique »
http://www.secusys.com/
hhttp://abcdelasecurite.free.fr
ttp://websec.arcady.fr/ : (il n'est pas accessible actuellement)
http://terroirs.denfrance.free.fr/ : site à l'origine dédié à la cuisine mais avec une partie sécurité informatique très détaillée et complète.

http://www.securite.teamlog.com
http://www.e-prevention.ch/web
http://ixus.net : site sur la sécurité plutôt unix/linux avec partie juridique. Liste des ports très complète. Glossaire informatique de trigrammes très complet. Liste des chevaux de Troie actualisées.
http://www.linuxsecurity.com/
http://users.swing.be/michel.hoffmann/ : faq sécurité informatique
http://fr.trendmicro-europe.com/ : alertes virales.
http://perso.wanadoo.fr/pc.network/ : site spécialisé sur les chevaux de Troie.
http://www.cookiecentral.com/ : site dédié aux cookies et dérivés.
http://ibelgique.ifrance.com/secur/
http://www.cameleon.org/ : nouvelle version en préparation
http://impertinence.com/ : partie sécurité pas remise à jour depuis 2000.

Sites anglo-saxons :

http://anonymizer.com/
http://infosyssec.net/ : The Security Portal for Information System Security Professionals
http://securityfocus.com/
http://www.tom-cat.com/
http://www.spychecker.com
http://www.hideaway.net/home/public_html/index.php
http://www.spywareinfo.com/~merijn/
http://www3.ca.com/virusinfo/ : virus information center.
http://www.sans.org : SysAdmin, Audit, Network, Security
http://www.bigbrotherinside.org/ non réactualisé depuis 2000, du même auteur que « anonymat.org ».
http://searchsecurity.techtarget.com/
http://www.spyware.co.uk/
http://www.pestpatrol.com/
http://www.insecure.org/

Autres :

http://www.websense.com :
http://www.websense.com/company/news/research/Emerging_Threats_2003_EMEA-fr.pdf : Menaces Internet émergentes 2003 : étude réalisée par Websense et Infosécurité Europe 2003.
http://rsf.fr/ : reporters sans frontières, dossier Internet sous surveillance.

http://www.junkbusters.com
http://caspam.org/ : site dédié au spam

Échelon :
www.europarl.eu.int/committees/echelon_home.htm : commission temporaire sur le système d'interception échelon avec les rapports de la STOA.

http://www.assemblee-nat.fr/rap-info/i2623.asp : rapport de l'Assemblée Nationale sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale.
http://www.stoa.org/ : rapports de la STOA commandé par le Parlement Européen sur Échelon.
http://www.fas.org/irp/eprint/ic2000/ic2000.htm : Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office) on the development of surveillance technology and risk of abuse of economic information.
http://reseau.echelon.free.fr/reseau.echelon/
http://echelononline.free.fr/

NGSCB et TCG :
http://www.trustedcomputing.org : site du projet TCPA
http://www.laboratoire-microsoft.org/articles/win/ngscb/ : présentation de Microsoft du projet NGSCB (Palladium)
http://www.microsoft.com/france/securite/entreprises/ngscb/livresblancs/default.asp
http://www.microsoft.com/france/securite/entreprises/ngscb/default.asp : les spécifications du NGSCB / Palladium
http://perso.club-internet.fr/vadeker/humanite/geopolitique/microsoft_palladium_tcpa_presses.html : Revue de presse sur l'initiative Palladium de Microsoft et du concept d'informatique de confiance TCPA (Trusted Computing Platform Alliance).
https://www.trustedcomputinggroup.org/home : TCG
http://www.lebars.org/sec/ : information sur Palladium et TCPA.

http://www.wi-fi.org/OpenSection/index.asp
Les applets Java et les contrôle Active X hostiles par Alexandra Brumet : Systèmes et Sécurité, volume 5 n°4 Paris 1999.

http://www.renseignementsgeneraux.net/
http://www.w3.org/P3P/ : platform for privacy preferences

http://whatis.techtarget.com (définition)
http://www.kitetoa.com/

http://www.commentcamarche.net/ : site de vulgarisation informatique assez complet.
http://memoclic.com : site informatique non spécialisé (actualités, logiciels, matériels…).
http://www.p2p4.com/

http://www.hsc.fr : cabinet de consultant avec des cours et études. Hervé Schauer Consultants
http://www.lavasoftusa.com/ : éditeur de Ad-aware
http://www.safer-networking.org/ ou http://security.kolla.de/ : éditeur de spybot Search & Destroy

http://www.ami.com/ : American Megatrends
http://cexx.org

Administration, organisations institutionnelles et associations

France et Europe :

http://www.certa.ssi.gouv.fr : Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques. C'est l'un des CERT (Computer Emergency Response Team) français participant au réseau mondial des CERT. Il est dédié à l'administration française et rattaché à la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) au sein du secrétariat général de la Défense Nationale (SGDN) dépendant directement du premier ministre.
Publie des avis et bulletins d'alertes. Sa création date du 19 janvier 1999.
http://www.ssi.gouv.fr/fr/index.html : Serveur thématique sur la sécurité des systèmes d'information. (rattaché au Premier Ministre).
http://www.ssi.gouv.fr/fr/dcssi/index.html : le site de la DCSSI (Direction centrale de la sécurité des systèmes d'information). La DCSSI a remplacé le service central de la sécurité des systèmes d'information (SCSSI) créé en 1984.
http://www.art-telecom.fr/ : Autorité de Régulation des Télécommunications. Organisme qui a trois domaine de compétence : domaine de l'interconnexion, les colocalisations, la mise à niveau des réseaux câblés.
http://www.cnil.fr : Commission Nationale de l'Informatique et des Libertés. Veille au respect des lois françaises concernant l'informatique, ainsi qu'à la légalité des fichiers nominatifs et de leur utilisation - application de la loi 78-19 de janvier 1978 relative à l'informatique, aux fichiers et aux libertés -
http://www.senat.fr/rap/ : les rapports du Sénat sur l'espace et les renseignements militaires et sur les politiques de renseignement.
http://www.assemblee-nat.fr/
http://www.dgse.org/ : Direction Générale de la Sécurité Extérieure. Groupe d'étude indépendant sur le renseignement français.
http://www.inria.fr/ : Institut National de Recherche en Informatique et en Automatique.
http://www.loria.fr/ : laboratoire lorrain de recherche en informatique et ses applications.

https://www.clusif.asso.fr/ : Club de la Sécurité des systèmes d'information français.
http://www.iabfrance.com/ : Interactive Advertising Bureau, division locale française.
http://www.ipsos.fr/

http://www.vie-privee.org : Fédération Informatique et Libertés (FIL)
http://www.lsijolie.net/ : site d'archive car aujourd'hui sur vie-privée.org
http://www.iris.sgdg.org/ imaginons un réseau Internet solidaire. Association loi 1901.
http://www.edri.org/ : (European Digital Rights) lobby pour la protection de la vie privée numérique (EDRi). C'est l'association Iris qui prend part à ce projet en France.

États-Unis :

http://www.cert.org : (Computer Emergency Response Teams) centre d'expertise de sécurité Internet, cellule d'alerte sur la sécurité informatique. Centre d'étude et de recherche lié aux problèmes de sécurité informatique. Créé en décembre 1988 par la DARPA suite à la diffusion d'un virus qui bloquera, en novembre de la même année, 10 % des ordinateurs connectés au réseau.

http://www.ietf.cnri.reston.va.us/home.html : The Internet Engineering Task Force
http://www.ciac.org/ciac/ : Computer Incident Advisory Capability (US department of Energy)
http://www.nsa.gov/ : National Security Agency
http://www.cia.gov/ : Central Intelligence Agency
http://www.fbi.gov/ : Federal Bureau of Investigation
http://www.darpa.mil/ : Defense Advance Research Project Agency. Cette agence américaine dépend du secrétariat de la défense américaine. Elle est à l'origine, entre autre, de l'ARPANET.

http://www.epic.org/ Electronic Privacy Information Center : centre d'information sur la vie privée électronique, défend la vie privée numérique.
http://www.aclu.org/ : American Civil Liberties Union : association de défense des libertés civiles et de l'Internet. Renseignement sur les projets gouvernementaux ou de services spéciaux comme Echelon et Carnivore.
http://www.privacyfoundation.org/ : association de défense pour la vie privée située dans le Colorado (US). Beaucoup de lien de sites américains.
http://www.first.org : Forum of Incidence Response and Security Team
http://www.privacy.org/ et http://www.privacyinternational.org/
http://privacy.net/ : the consumers information organisation
http://www.cdt.org/ : Center for Democracy and Technology
http://www.dfn.org/ : Digital Freedom Network
http://www.eff.org/ : (Electronic Frontier Foundation) "defending freedom in the digital world".
http://foi.com/ et http://privacy.net/ : the consumer information organization

Sites juridiques et documents officiels :

www.cnil.fr : Commission Nationale de l'Informatique et des Libertés.

- http://www.cnil.fr/frame.htm?http://www.cnil.fr/textes/ttext.htm : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

http://www.legifrance.gouv.fr/ : service public de la diffusion du droit

- http://www.legifrance.gouv.fr/WAspad/UnCode?code=CPENALLL.rcv : Code Pénal
- http://www.legifrance.gouv.fr/WAspad/UnCode?code=CTRAVAIL.rcv : Code du Travail
- http://www.legifrance.gouv.fr/texteconsolide/PCEAR.htm : Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.
- http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0100032L : Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne

http://www.droit-technologie.org/

- http://www.droit-technologie.org/legislations/CPVP_avis_ecommerce_221100.pdf : avis de la commission pour la protection de la vie privée.
- http://www.droit-technologie.org/1_2.asp?actu_id=758 : article sur l'application de la directive de 95.

- http://www.droit-technologie.org/legislations/rapport_evaluation_directive_vie_privee_9546_FR.pdf : rapport de la commission sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)

www.industrie.gouv.fr :
- http://www.lsi.industrie.gouv.fr/observat/innov/lsi/index.html : loi sur la société de l'information

http://www.echr.coe.int/ : Cour Européenne des droits de l'homme
- http://www.echr.coe.int/Convention/webConvenFRE.pdf : convention européenne des droits de l'homme, 4 novembre 1950.

https://wcm.coe.int/rsi/cm/index.jsp : Conseil de l'Europe, Comité des ministres
- http://cm.coe.int/ta/rec/1989/f89R2.HTM : Recommandation n° R (89) 2 du Comité des Ministres aux Etats membres sur la protection des données à caractère personnel utilisées à des fins d'emploi.

http://europa.eu.int/ : site de l'Union Européenne
- http://europa.eu.int/ISPO/legal/fr/dataprot/directiv/direct.html : directive 95/46/CE
- http://europa.eu.int/eur-lex/pri/fr/oj/dat/2002/l_201/l_20120020731fr00370047.pdf : directive 2002/58/CE

http://www.g8j-i.ca/french/chair.html : Réunion des ministres de la Justice et de l'Intérieur du G8, Mont-Tremblant, 13 et 14 mai 2002.
http://www.g8j-i.ca/french/doc2.html : Recommandations sur le dépistage des communications électroniques transfrontalières dans le cadre des enquêtes sur les activités criminelles et terroristes.
http://www.g8j-i.ca/french/doc3.html : Principes relatifs à la disponibilité des données essentielles au maintien de l'ordre public.

www.infojuris.com
http://www.foruminternet.org/ : forum des droits sur l'Internet
http://www.droitdunet.fr/ : le service pratique des droits sur l'Internet, vulgarisation.

Listes :

http://terroirs.denfrance.free.fr/p/frameset/09.html :
liste des spywares et key loggers en fonction des logiciels pouvant les retirer.
Liste des logiciels comportant des spywares
Liste des bho
Liste des key loggers
Liste des web bug
http://www.secuser.com/information/spywarelist14.zip : liste de spyware
http://www.tom-cat.com/spybase/index.html : liste de spyware
http://www.securiteinfo.com/conseils/portstroyens.shtml ou http://www.simovits.com : liste des ports troyens
http://www.onctek.com/trojanports.html : liste de chevaux de Troie
http://ixus.net/modules.php?name=Ixus_Nettools&d_op=Trojans : liste de chevaux de Troie