L'ANONYMAT SUR INTERNET

1 LE RESPECT DE LA VIE PRIVEE 2

1.1 DROIT DES PERSONNES : 2
1.2 DÉCLARATION DES FICHIERS : 2

2 TRACES LAISSEES 3

2.1 TRACES SUR VOTRE ORDINATEUR : 3
2.2 TRACES SUR INTERNET : 4
2.2.1 Informations fournies par le navigateur : *4*
2.2.2 Cookies : *4*
2.2.3 Mouchards : *5*
2.3 ESPIOGICIELS (LOGICIELS ESPIONS) : 5

3 RESTER ANONYME OU CONFIDENTIEL 6

3.1 PROTÉGER SES DONNÉES PERSONNELLES : 6
3.1.1 Cryptage symétrique et asymétrique : *6*
3.1.2 Cryptage RSA *6*
3.1.3 Cryptage PGP *8*
3.1.4 Stéganographie *8*
3.2 SURFER ANONYME : 9
3.2.1 Le serveur de proxy *9*
3.2.2 Des anonymiseurs professionnels *9*
3.2.3 Un proxy personnel *10*

4 DOCUMENTATIONS 11

4.1 INFORMATIONS SUR LES DROITS DES PERSONNES : 11
4.2 ACRONYMES : 11

1 LE RESPECT DE LA VIE PRIVEE

La sécurité informatique est liée essentiellement aux **données,** elle a pour but de protéger les richesses de l'entreprise. Les données doivent être sécurisées contre les pertes, modifications, accès non autorisé, vol…

Le respect de la vie privée est lié à la **personne**, même en entreprise, celle-ci a droit à un minimum d'anonymat.

1.1 Droit des personnes

Selon la législation du pays, les personnes bénéficient de droits plus ou moins étendus, notamment en ce qui concerne les principes de protection des données personnelles reconnues par les législations européennes et tout particulièrement en France par la loi du 6 janvier 1978. Malheureusement, depuis le 11 septembre 2001, plusieurs pays restreignent fortement ces droits en particulier le LSQ en France et il faudra attendre les divers recours contre ces lois (droit de l'homme, constitution, liberté d'expression…).

Concernant la mise en fichier, en France on dispose :

- D'un droit à l'information préalable
- D'un droit de curiosité
- D'un droit d'accès direct et indirect
- D'un droit de rectification et d'opposition
- D'un droit à l'oubli.

La consultation du courrier électronique de ses employés, pour des raisons de sécurité, n'est par exemple tolérée qu'après les en avoir informés. Ceux-ci restent cependant privés et sont difficilement opposables judiciairement aux personnes concernées.

Un employeur peut sanctionner pour rupture de contrat un salarié qui utilise Internet à des fins personnelles, et ce quelque soit le site visité, au titre qu'il est payé pour exécuter certaines tâches. L'employeur a tout à fait le droit de contrôler et de surveiller l'activité des salariés. En revanche, il ne pourra pas utiliser les informations récupérées comme mode de preuve s'il n'a pas informé les salariés que l'utilisation d'Internet peut être contrôlée et utilisée dans le cadre d'une procédure disciplinaire. Attention, lorsqu'on parle d'intercepter les mails, il s'agit de vérifier les destinataires ou les expéditeurs des mails mais en aucun cas de lire le contenu du mail. Si c'était le cas, l'employeur commettrait un délit prévu à l'article 226-15 alinéa 2 du nouveau Code pénal qui protège le secret des correspondances

Sur le règlement intérieur, l'employeur peut faire apparaître effectivement que l'utilisation d'Internet à des fins personnelles est interdite et pourra donner lieu à des sanctions disciplinaires. Sur le contrat de travail, on trouvera plutôt des mentions avertissant le salarié que le matériel et les ressources mis à disposition devront être réservées à un usage strictement professionnel et que le respect de cette condition pourra faire l'objet de contrôle et que les mails pourront être utilisés comme preuve lors d'une procédure disciplinaire

1.2 Déclaration des fichiers

La loi du 6 janvier 1978 impose à toute personne mettant en œuvre un traitement automatisé de données nominatives d'en faire une déclaration préalable auprès de la CNIL. On

considère comme « nominatives » toutes informations permettant l'identification de personnes physiques auxquelles elles s'appliquent.

Cette loi confère aux personnes concernées un droit d'information préalable, un droit d'accès, de rectification et d'effacement. La déclaration peut se faire en ligne sur le site de la CNIL ***www.cnil.fr*** .

Il existe des normes simplifiées pour certaines déclarations : gestion des membres d'une association 1901, mise en œuvre d'un PABX …

Recommandations de la CNIL pour les traitements accessibles sur Internet :

- Information préalable et consentement éclairé des personnes.
- Mention de l'interdiction de capture à des fins commerciales ou publicitaires.
- Accès par lien aux dispositions légales.

2 TRACES LAISSEES

En entreprise, le réseau local étant connecté à Internet, un indispensable contrôle des communications est réalisé. La loi impose parfois l'archivage, en vue d'une procédure judiciaire future, des transactions effectuées.

2.1 Traces sur votre ordinateur

Les opérations effectuées sur votre ordinateur laissent d'innombrables traces, exemple pour un PC sous Windows :

Traces	Effacement
Derniers fichiers ouverts : - démarrer/documents... - \windows\recent NT : \winnt\profiles\ " user "\recent	 - clicD/barre, prop., programme, menu.., effacer - effacer le rep. \Windows\recent - effacer \récent (pour " admin.. " récent est caché !)
Derniers fichiers modifiés : Explorateur, outils/rechercher/fichier/date...	
Fichiers temporaires : - c:\temp, c:\windows\temp - \programfiles\m$office\office\gestionnaire office	- Rechercher puis effacer *.tmp ou ~*.*
Utilisation de logiciels : - chercher *.log puis éditer...	
Word : " fichier ", dernier document ouvert...	" outils ", option, général, décocher " derniers fichiers utilisés "
OFFICE97… : les documents créés contiennent un GUID (adresse MAC du PC..). Visu possible par wordpad Test par ***http://security.pharlap.com/regwiz/index.htm***	- W98 : regsvr32.exe -u c:\windows\system\regwizc.dll - Outil sur ***http://www.vecdev.com/guideon.html***
Base de registre : - Regedit, rechercher MRU (Most Recently Used)	

- Proprio PC : \HKLM\soft.\m$\win.\curr.ver	- Modif Identification et owner possible
IE : - Base reg \HKCU\soft.\m$\ie\typed URLs - Temporaire en C:\windows\temporary internet files - Historique en C:\windows\historique - Favoris en C:\windows\favoris IE5 : si saisie semi-auto, identifiant et pwd mémorisés !	 - "affichage", option, avancées, décocher utilisation zone - IE5 : outils, option Internet, supprimer les fichiers… Ou : outils, opt i, avancé, sécurité=cocher "vider .." - Outils, option Internet, effacer historique. Ou : Raz nb jours de conservation historique - Faire outils, option Internet, contenu, saisie semi-auto, effacer les formulaire et décocher « nom utilisateur… ».
NETSCAPE : - Temporaire en C:\prog.files\nets.\nav.\cache - Historique : Ctrl-H ou fichier Netscape.HST Historique txt dans \netscape\users\default**pref.js** - Favoris : fichier Bookmark.htm	 - édition, préférences, navigateur…
EFFACEMENT DE FICHIERS : - corbeille (pas d'effacement véritable !) - effacement (récupération parfois possible)	 - vider régulièrement (= effacement) - utiliser un logiciel de destruction.

2.2 Traces sur Internet

2.2.1 Informations fournies par le navigateur :

Lors de la présentation de votre requête http au site visité, plusieurs informations sont fournies à ce site :

REMOTE_HOST = ppptc14.infini.fr
REMOTE_ADDR = 212.208.100.74
HTTP_USER_AGENT = Mozilla/4.05 [fr] (Win95; I)
HTTP_REFERER = http://www.cnil.fr/traces/demonst/demo.htm

- Adresse DNS de votre FAI.
- Adresse IP de votre machine.
- Navigateur utilisé et système d'exploitation.
- URL de la page précédente.

Les adresses servent à retourner la réponse, le navigateur (ici Netscape) permet éventuellement de vous envoyer une page adaptée à celui-ci…

Consulter ***www.cnil.fr/traces*** .

2.2.2 Cookies :

Un cookie est une chaîne de caractère envoyé par le serveur par insertion d'une directive dans l'en-tête du message de réponse HTTP dont la syntaxe est la suivante :

Set-Cookie : Nom=valeur; expires=date; path=chemin, domain=nom_domain; secure

Le cookie est déposé sur votre disque dur, via votre navigateur, afin normalement d'accélérer ou d'autoriser votre prochaine visite. On trouvera des infos sur les cookies à ***www.epic.org/privacy/internet/cookies***

Des logiciels permettant le tri des cookies sont disponibles : « cookie crusher » sur ***www.thelimitsoft.com*** et « cache & cookiewasher » sur ***www.webroot.com***

En règle générale, on préférera limiter les cookies à la session en cours ou n'accepter que vers le serveur qui les émet :

- **IE :** outils, option internet, sécurité, personnaliser le niveau, cookies : autoriser les cookies par session et refuser qu'ils soient stockés sur le PC. Les cookies sont enregistrés dans le répertoire \windows\cookies.
- **Netscape :** édition, préférence, avancées, cookies : accepter uniquement les cookies qui sont renvoyés au serveur d'origine. Les cookies sont sauvegardés dans le fichier cookies.txt. Si on désire effacer ce fichier à chaque démarrage on pourra placer dans autoexec.bat la commande *copy modele.txt cookies.txt* (en précisant le chemin), le fichier modele.txt doit contenir les 3 premières lignes de cookies.txt (jusqu'à *do not edit*)

2.2.3 Mouchards :

Un « Web bug » peut être inséré dans n'importe qu'elle page HTML ou même dans des documents Bureautique. Il s'agit d'une ligne de commande en HTML, identique a celle utilisée pour appeler une image sur un serveur. Sauf qu'il n'y a pas d'image sur le serveur, mais un script qui déclenche la collecte d'informations. Le serveur a accès à toutes sortes d'informations vous concernant Il peut savoir par quel fournisseur d'accès vous passez et aussi renvoyer un cookie, qui permettra ensuite d'analyser votre utilisation du document. En combinant cookies et Web bugs, les possibilités s'étendent. Il n'est pas évident de savoir quels renseignements peuvent être obtenus de la sorte, cela dépend de la configuration de l'ordinateur. Bien souvent, en recoupant les informations avec une base de données bien fournie, votre identité peut être retrouvée. Ensuite vos habitudes sur un site peuvent être étudiées, vos visites comptabilisées et vos heures de passage de même. Bref, votre profil peut être établi pour une utilisation commerciale. Les équipes de marketing sont en effet friandes de ces techniques et les newsletters sont connues pour héberger ces Web bugs

2.3 Espiogiciels (Logiciels espions)

Plusieurs logiciels connus se permettent de renvoyer vers l'éditeur des informations concernant l'usage du logiciel mais aussi sur les habitudes ou la configuration de l'utilisateur, et ceci au mépris de la loi « informatique et liberté ». Il s'agit souvent de « freewares » qui trouvent ainsi une source de revenus mais pas toujours !

Ces logiciels sont appelés ***« spyware »***, ils ne posent pas, à priori, de problème de sécurité mais plutôt celui du respect de la vie privée.

Exemples : Real Networks (requête vers l'éditeur à chaque insertion de CD-audio avec n° GUID, adresse mail…), CuteFTP…

Une liste des programmes suspects est disponible sur ***www.lavasoft.com***

Logiciel pour supprimer des espions recensés : Ad-Aware et optout.exe sur ***//grc.com***

3 RESTER ANONYME OU CONFIDENTIEL

3.1 Protéger ses données personnelles

La protection de l'intégrité de vos données sera effectuée par un antivirus et la confidentialité par un logiciel de cryptage.

3.1.1 Cryptage symétrique et asymétrique :

Une clé est une valeur qui est utilisée avec un algorithme cryptographique pour produire un texte chiffré spécifique. Les clés sont, à la base, de très grands nombres. La taille d'une clé se mesure en bits; et le nombre qui peut être représenté par une clé de 1024 bits est vraiment immense. En matière de cryptographie, plus la clé est grande, plus le chiffrement est sûr.

La cryptographie conventionnelle est symétrique : on utilise la même clé pour crypter et pour décrypter. Très efficace, rapide et sure cette méthode pose le problème de la distribution de la clé dans un réseau. Exemple : DES et Triple DES (basé sur des permutations…).

La cryptographie à clé publique utilise 2 clés liées, le destinataire de documents génère une paire de clés, distribue sa clé publique à celui qui doit lui transmettre un message (ou la laisse à disposition sur un serveur). Cette clé sera utilisée par l'émetteur pour chiffrer son message et seule la clé privée du destinataire permettra de déchiffrer ce message. (voir explication de RSA plus loin).

Cependant, la taille d'une clé publique n'est absolument pas comparable avec la taille des clés secrètes employées en cryptographie conventionnelle. Une clé conventionnelle de 80 bits offre une sécurité équivalente à celle d'une clé publique de 1024 bits. Une clé conventionnelle de 128 bits équivaut à une clé publique de 3000 bits. Encore une fois, plus grande est la clé, plus grande est la sécurité, mais les algorithmes utilisés pour chaque type de cryptographie sont très différents, et donc, comparer les tailles de clés revient à comparer des pommes et des oranges.

Les clés les plus grandes resteront cryptographiquement sûres pour une plus longue période (Si ce que vous chiffrez doit rester caché de nombreuses années)
Ronald Rivest, Adi Shamir et Leonard Adleman

3.1.2 Cryptage RSA

L'algorithme de chiffrement RSA *(du nom de ses inventeurs : ronald Rivest, adi Shamir et leonard Adleman)* est fondé sur notre ignorance : aucune méthode de décomposition des nombres en facteurs premiers n'a été découverte à ce jour.

Les nombres premiers ne sont divisibles que par 1 et par eux-mêmes, et sont en nombre infini, comme l'a démontré Euclide il y a 2300 ans. Tout nombre entier peut être décomposé, et ce de manière unique, en un produit de nombres premiers. Ainsi, 4410 par exemple peut s'écrire $2x3^2x5x7^2$. Or, si la multiplication des nombres premiers est une opération très facile, trouver les diviseurs premiers d'un nombre N donné n'a pas de solution connue. C'est sur ce principe qu'est basé l'algorithme de chiffrement. Il est bien

sur possible, grâce aux ordinateurs, de tenter la force brutale, c'est à dire de diviser N par tous les nombres inférieurs à sa racine carrée. Mais cette solution sauvage n'est plus utilisable avec de grands nombres. Ainsi, en 1994, il a fallu recourir à des milliers d'ordinateurs en réseau pour factoriser un nombre de 129 chiffres.

Avant d'expliquer comment fonctionne RSA, rappelons la notion de "congruence". On dit qu'un nombre a est congru à b modulo n, ce que l'on note $a \equiv b \pmod{n}$ lorsqu'il existe un entier k satisfaisant l'équation a = b + kn. Ainsi, $26 \equiv 5 \pmod{7}$, car 26/7 donne comme reste 5.

RSA utilise la procédure à clé publique, un des correspondants crée deux clés : l'une publique qu'il diffuse à tout le monde, l'autre privée qu'il garde secrète. Ces clés sont reliées entre elles par une relation mathématique impossible à découvrir. N'importe qui peut utiliser la clé publique pour coder un message, mais seul celui qui possède la clé privée sera capable de le déchiffrer. Le calcul de ces clés s'effectue de la façon (simplifiée) suivante :

- On prend deux grands nombres premiers **p** et **q**, puis on calcule le produit **N = pq**.
- Ensuite, on choisit arbitrairement un nombre **e** premier avec **(p-1)(q-1)**.(c'est à dire que ces 2 nombres n'ont que 1 comme diviseur commun, **e** n'est pas obligatoirement premier)
- Le nombre **N** et le nombre **e** représentent la clé publique.
- La clé privée de décryptage, notée **d** est calculée par la formule $\mathbf{ed \equiv 1 \bmod ((p-1)(q-1))}$, facilement calculable par l'algorithme d'Euclide.

Pour coder un message, qui doit être sous forme numérique, on le découpe en tranches $\mathbf{M_1, M_2 ... M_n}$, dont la taille est de l'ordre de **N**. Chaque tranche $\mathbf{M_i}$ est alors codée par la formule $\mathbf{C_i \equiv M_i^e \bmod(N)}$, dans laquelle **Ci** représente la partie codée de la tranche $\mathbf{M_i}$.

Le déchiffrement s'effectue ensuite en appliquant la formule $\mathbf{M_i \equiv C_i^d \bmod (N)}$.

Il faut bien comprendre que RSA s'appuie seulement sur le fait que nous ne connaissons pas de méthode pour retrouver p et q (ce qui permettrait de calculer la clé secrète d) à partir du nombre N, qui lui est public.

Exemple de codage avec l'algorithme RSA :

- Prenons deux nombres premiers soit: p=7 et q=17
- Calculons N = p*q = 119.
- Choisissons arbitrairement un nombre premier avec (p-1)(q-1) = 6*16 = 96 soit par exemple e=5.
- Calculons la clé secrète par la formule $ed \equiv 1 \bmod ((p-1)(q-1))$ en utilisant 1'algorithme d'Euclide. On obtient d = 77.
- La clé publique est 119 et 5. La c1é privée est 77.
- Les nombres p et q ne sont plus utilisés.
- Soit par exemple à coder le nombre 19.
- Posons $C \equiv 19^5 \bmod (119)$ soit C = 66.
- Pour déchiffrer le message, calculons $M \equiv 66^{77} \bmod (119)$, ce qui nous donne à nouveau M = 19.

Dans la réalité, les nombres p et q sont choisis très grands (jusqu'à une centaine de chiffres). On dispose de certaines méthodes pour les obtenir. Il existe également des techniques pour simplifier les calculs de codage et de décodage. Dans notre exemple il ne serait pas nécessaire de calculer une valeur telle que 66^{77} . Il serait possible de calculer de faibles puissances de 66 d'effectuer les opérations de modulo et ainsi de suite pour ne jamais avoir à manipuler d'aussi grands nombres.

3.1.3 Cryptage PGP

PGP combine à la fois les meilleures fonctionnalités de la cryptographie conventionnelle et de la cryptographie à clé publique (RSA).

Le cryptage PGP effectue les opérations suivantes :

- Compression du document.
- Cryptage avec une clé de session symétrique du document.
- Cryptage de la clé de session avec la clé publique du destinataire.
- Transmission de l'ensemble.

Compression : la compression de données économise du temps de transmission par modem et de l'espace disque et, ce qui est plus important, renforce la sécurité cryptographique. La compression réduit les redondances dans le document, ce qui augmente grandement la résistance à la cryptanalyse. (Les fichiers qui sont trop petits pour être compressés ou qui ne se compressent pas bien ne sont pas compressés.)

Clé de session : PGP crée ensuite une *clé de session,* qui est une clé secrète qui ne sert qu'une fois. Cette clé est un nombre aléatoire généré à partir des mouvements aléatoires de votre souris et des touches du clavier sur lesquelles vous tapez. Cette clé de session est utilisée par un algorithme de chiffrement conventionnel très sûr et rapide qui chiffre le document compressé.

Transmission : Une fois que les données sont chiffrées, la clé de session est elle-même chiffrée avec la clé publique du destinataire. Cette clé de session chiffrée par la clé publique est transmise avec le document chiffré au destinataire.

Le déchiffrement fonctionne de la manière inverse. La copie de PGP du destinataire utilise sa clé privée retrouver la clé de session temporaire, que PGP utilise ensuite pour déchiffrer le document de manière conventionnelle.

La combinaison des deux méthodes de chiffrement associe la commodité du chiffrement à clé publique avec la vitesse du chiffrement conventionnel. Le chiffrement conventionnel est environ 1000 fois plus rapide que le chiffrement à clé publique. Le chiffrement à clé publique fournit quant à lui une solution aux problèmes de distribution de la clé et de transmission des données. Utilisées toutes les deux, la performance et la distribution de la clé sont améliorées sans aucun sacrifice sur la sécurité.

3.1.4 Stéganographie

La stéganographie est la technique permettant de cacher une information dans un message anodin (texte dans une image…). Exemple de logiciel : Invisible secret Pro sur ***www.east-tec.com/ispro*** …

3.2 Surfer anonyme

Les traces les plus importantes sont chez votre fournisseur d'accès, un FAI gratuit peut récupérer votre n° de téléphone (faire **3651** avant de composer le n° pour que celui-ci reste secret) afin de mettre un nom sur votre « pseudo »…

L'IP-spoofing (usurpation d'une adresse IP) est illégale et délicate.

3.2.1 Le serveur de proxy

Un serveur proxy, aussi appelé serveur mandataire, peut être situé sur tout point du réseau mais l'est généralement chez votre fournisseur d'accès. Le serveur proxy est généralement associé à un « cache ». Lorsque vous exécutez une requête vers un serveur du réseau, le proxy en question vérifie si la requête est autorisée (fonction *firewall*, black list…) et si la même requête a déjà été faite précédemment. Si ce n'est pas le cas, il la lance pour vous, et vous transmet son résultat - par exemple la page HTML demandée - après l'avoir enregistré sur son disque dur (fonction cache). Ainsi, si vous ou un autre client du fournisseur d'accès lance la même requête peu de temps après, c'est le serveur de proxy qui y répondra en allant la chercher simplement sur son disque dur. D'où un gain considérable en temps et une économie de bande passante pour le fournisseur d'accès.

Cette situation implique deux conséquences :

1. C'est la trace du proxy qui figurera dans le fichier d'audit du serveur Internet que vous avez contacté,
2. Le proxy, lui, pourra très bien conserver l'intégralité de l'historique de toutes vos requêtes. Si le proxy est situé dans votre entreprise, la configuration est la même que dans le cas du firewall ci-dessus : l'administrateur du proxy peut reconstituer toutes vos transactions. S'il est chez votre fournisseur d'accès, c'est ce dernier qui dispose de ces informations.

Imaginons qu'un internaute se livre à des opérations qui portent atteinte à des personnes (diffamation, injure, propos racistes, etc.). Le serveur auquel se plaindrait la victime ou par lequel transiteraient les paquets qui causent des dommages à autrui, pourrait très bien informer votre fournisseur d'accès - dénoncer une infraction est une obligation légale - qui pourrait alors vous sanctionner en annulant votre abonnement. La victime pourrait aussi faire appel à la justice et c'est un magistrat qui rapprocherait le journal des connexions du fournisseur d'accès et le fichier d'audit du serveur sur lequel les malversations auraient eu lieu.

3.2.2 Des anonymiseurs professionnels

Certains sites vous proposent de jouer le rôle d'anonymiseur. Concrètement, vous vous connectez sur un site web anonymiseur A. Il vous propose de taper l'adresse d'un autre serveur B à l'intérieur d'une page web dans une boîte de saisie. Puis le serveur A envoie la requête vers B, lequel transmet à A le résultat de sa requête. A redirige alors sur vous ce résultat. Le fichier d'audit de B contient donc l'adresse IP de A, et seul le fichier

d'audit de A contient votre adresse IP. Pour vous identifier, l'administrateur du serveur B devrait demander au serveur A un extrait de son fichier d'audit, ce que A, a priori, refuserait de faire, c'est du moins ce que ce type de serveurs annoncent. On peut tout de même observer que si les proxy publics sont toujours en fonction c'est parce que la majorité d'entre-eux collabore avec les victimes de « plaisanteries ».

Il faut noter tout de même que si lui, l'anonymiseur, vous a tracé, il est en mesure de savoir à quoi vous vous intéressez et, mieux encore, il sait que vous souhaitez rester anonyme.

Certains sites permettent une navigation anonyme : ***www.anonymizer.com*** , ***www.privacyx.com***, ***www.secuser.com/anonymiser*** .

Ces sites étant généralement gratuit, ils sont généralement assez lents et vous gratifient de publicités. De plus on peut sérieusement envisager que pour se financer ils revendront les données statistiques qu'ils auront récoltés ! Un proxy personnel pourra être plus efficace.

3.2.3 Un proxy personnel

On utilisera un logiciel gratuit qui s'appelle *Multiproxy* et que l'on peut télécharger depuis ***www.multiproxy.org***. Ce logiciel s'installe entre vos logiciels de navigation et votre connexion et transmet vos requêtes à des serveurs *proxy* anonymes. Au lancement, le logiciel cherche dans une liste prédéfinie de *proxies* anonymes lesquels sont disponibles. Il choisira ceux qui répondent le plus vite. Une seule modification desdits logiciels pour leur dire de passer par un proxy et on jouera le surfeur masqué. Il n'est pas dit que Multiproxy fonctionne pour tous les protocoles, notamment HTTPS (Sécurisé) et Socks. Mais pour HTTP et FTP les plus couramment utilisés, ce sera parfait.

Configuration de *Multiproxy* :

- Cliquez sur le bouton **Options.** L'onglet **General** vous offre, dans la case **Accept connections on port,** le choix du port sur lequel Multiproxy «écoutera vos requêtes (par défaut, Le port 8088). On évitera les ports utilisés par les services courants: 21, 25, 80, 110... Au cas Où, choisissez une valeur entre 8000 et 65536, pour être tranquille. Cochez la case **Test all servers on start-up** pour que le programme vérifie la disponibilité des *proxies* au démarrage, et **Start minimized** Si vous voulez qu'il se glisse dans la barre des tâches. La plupart des options par défaut sont bonnes. Vérifiez juste dans la rubrique **Connect** via que le bouton **Anonymous proxies only** est activé, pour ne pas risquer d'utiliser un *proxy* non anonyme.
- Dans **Select next server,** activez **Rotate every** et choisissez le délai à l'issue duquel le programme change de serveur Idéal pour brouiller les pistes. Si vous n'êtes pas aussi inquiet, cochez juste **Next fastest available server,** afin que le *proxy* choisi soit le plus rapide du lot.
- Dans l'onglet **Proxy servers list** se trouvent les serveurs référencés par défaut dans le logiciel. Vous êtes libre d'en supprimer ou d'en rajouter. Un test vous informe de leur disponibilité (précédés d'un rond vert), de leur adresse IP et de leur temps de réponse (ping). Pour en supprimer un, cliquez dessus, puis activez le bouton **Menu** (en bas) et choisissez **Delete.** Mais la manœuvre la plus importante consiste à en rajouter de nouveaux. En vous rendant à

www.multiproxy.org/anon_list.htm vous découvrirez la liste régulièrement mise à jour des *proxies* anonymes, sur le modèle «adresse_du_proxy: port ».

- Enfin, dans l'onglet **Advanced options,** vérifiez que l'adresse 127.0.0.1 figure bien dans la rubrique **Allow connections from the following IP adresses only.** Son but : sécuriser Multiproxy. Explication: lorsque vous êtes connecté à Internet, le logiciel est accessible par votre adresse IP réelle. En limitant l'accès à certaines adresses IP vous vous gardez des intrusions. 127.0.0.1 est une adresse spéciale, dite « de boucle ». C'est le «moi-même» de l'IP: par elle, l'ordinateur s'auto-désigne. Si elle n'est pas dans la liste, cliquez sur **Add, saisissez 127.0.0.1** dans les deux lignes, et validez.

Configuration d'IE : Dans Internet Explorer, activez le menu **Outils, Options Internet, Connexion, Paramètres LAN.** Cochez la case **Utiliser un serveur Proxy** et indiquez **127.0.0.1** comme adresse, puis **8088** comme port (ou tout autre numéro de port que vous auriez assigné).

Configuration de Netscape : ouvrez le menu **Edition, Préférences, Avancées, Proxy,** activez le bouton radio **Configuration manuelle du Proxy,** cliquez sur **Afficher…** et entrez les mêmes renseignements dans toutes les lignes.

4 DOCUMENTATIONS

4.1 Informations sur les droits des personnes

- CNIL *(commission nationale de l'informatique et des libertés)* permet de vérifier les informations qu'un site peut obtenir sur vous lors de votre navigation (adresse, nom…) ***www.cnil.fr*** .
- Web sécurité ***http://websec.arcady.fr***
- Conseil de l'Europe ***www.coe.fr/cm/ta/rec/1999/f99r5.htm***
- AURIF *(association des utilisateurs de réseaux île de France)* ***www.aurif.fr***
- PGP *(cryptage)* ***www.pgp.com*** ***ou*** ***www.pgpi.com***
- Zataz *(info sur le piratage)* ***www.zataz.com***
- Privacy Foundation ***www.privacyfoundation.org***
- EPIC *(Electronic Privacy Information Center)* ***www.epic.org***
- Bug brother ***www.bugbrother.com***
- Loi LSI ***www.lsijolie.net***
- Junkbusters ***www.junkbusters.com/cgi-bin/privacy***
- Privacy.net (analyse de votre connexion…) ***http://privacy.net***

4.2 Acronymes

CNIL	: Commission Nationale de l'Informatique et des Libertés.
DES	: Data Encryption Standard (cryptage).
PGP	: Pretty Good Privacy (Protocole de cryptographie à double clé).
PKI	: Public Key Infrastructure (chiffrement).
RSA	: Rivest Shamir and Adleman (algorithme de cryptage à 2 clés).