La sécurité informatique

En guise de préambule …

La sécurité informatique du poste informatique (travail et/ou personnel) peut se résumer ainsi :

- *Prévention des attaques virales,*
- *Suppression des programmes espions et malveillants,*
- *Mise en œuvre d'une stratégie cohérente lors du choix des mots de passe,*
- *Assurance que le système dispose des dernières mises à jour logicielles,*
- *Sécurisation des logiciels installés sur la machine,*
- *Contrôle et blocage des tentatives d'intrusion,*
- *Archivage et stockage des données importantes,*
- *Appel au bon sens et à la réflexion lors de l'utilisation d'un équipement informatique et respect des règles de base de la protection.*

Malgré toutes les précautions mises en place, la sécurité informatique ressemble souvent à un jeu de « chat et de la souris » entre attaquants et défenseurs des systèmes informatiques.

De nombreuses interventions sur des machines contaminées auraient pu être évitées par une plus large diffusion et une meilleure connaissance des règles élémentaires de sécurisation d'un poste informatique.

Néanmoins, personne n'est à l'abri d'une attaque et la peur n'évite pas le danger …

1 LES RISQUES GENERAUX

1.1 Virus et programmes malicieux.

1.1.1 Virus

Un virus est un petit programme informatique conçu pour :

- Modifier à votre insu la façon dont votre ordinateur fonctionne,
- Se répandre systématiquement d'un ordinateur à un autre.

Les virus informatiques ne se génèrent pas de façon spontanée, quelqu'un les a écrit dans un but spécifique, et souvent dans l'intention de nuire.

Il est très important de souligner que la messagerie électronique est le principal vecteur de diffusion des virus, puisqu'elle permet la circulation rapide et simultanée des messages, mais surtout des pièces jointes qui peuvent être contaminées également.

Le virus ia pour but de se dupliquer et de se répandre de façon autonome, de préférence à votre insu en "s'accrochant" à un autre programme (votre tableur ou votre traitement de texte, par exemple) ou tout autre fichier programme exécutable. Lorsqu'un programme infecté est lancé le virus s'exécute. Souvent, il reste caché en mémoire vive, attendant un autre programme ou un autre disque à infecter.

De nombreux virus effectuent une action spécifique : affichage d'un message à une date précise ou suppression de fichiers après un certain nombre de lancements d'un programme infecté, etc.
La majorité des virus est cependant non destructrice et se contente d'afficher un message ou une image.
D'autres sont gênants, choisissant de ralentir votre ordinateur ou de modifier l'affichage à l'écran.

Une minorité est néanmoins réellement destructrice et bloque votre système, efface des fichiers, ou formate des disques.

1.1.2 Spyware

Contraction de « spy » et « software ».
Il s'agit d'un logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers, comme transmettre les données saisies grâce au clavier par exemple.

1.1.3 Adware

Contraction d'advertising spyware pour logiciel espion de publicité.
Les logiciels « adwares » inspectent les sites visités par les utilisateurs afin d'afficher des publicités ciblées, sous la forme de fenêtres « pop-up » ou de bannières.

Dans certains cas, ces espions se servent des informations collectées pour alimenter des bases de données commerciales. De nombreux programmes parrainés par de la publicité intègrent des « adwares », installés souvent à l'insu des utilisateurs.

1.1.4 Keyloggers

Il s'agit d'un type particulier de « spyware » spécialisé pour espionner les frappes au clavier sur l'ordinateur qui l'héberge, et pour les transmettre via Internet à une adresse où un pirate pourra les exploiter.
Un « keylogger » peut donc recueillir et transmettre vos mots de passe, codes de carte bancaire, intitulé sous lequel vous ouvrez une session...

Il est normalement indécelable pour l'utilisateur et n'apparaît généralement pas dans la liste des tâches s'exécutant sur la machine pour ne pas risquer d'être décelé.

1.1.5 Cheval de troie (Trojan)

Initialement un cheval de Troie désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu (en quelque sorte "déguisé" sous une fausse apparence), mais qui, une fois installé, exerçait une action nocive totalement différente de sa fonction "officielle".

Actuellement, le terme désigne à peu près tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spams, l'ouverture d'un accès pour un pirate...

La distinction entre cheval de Troie, spyware, keylogger, porte dérobée n'est donc souvent qu'une question de mot ou de contexte.

1.1.6 Rootkits

Les rootkits sont une variété de virus apparue d'abord dans le monde Unix/Linux puis, plus récemment, dans celui de Windows.
Ils peuvent être très difficiles à démasquer et parfois, à éradiquer. En effet, ils possèdent deux caractéristiques originales :

- d'une part, ils modifient en profondeur le fonctionnement du système d'exploitation (éventuellement son noyau)
- d'autre part, ils se rendent invisibles à ce système d'exploitation.

Ils peuvent même rendre invisibles divers autres parasites qu'ils auront installés : spyware, portes dérobée, cheval de Troie... et c'est ce qui constitue en général la raison majeure de leur existence.

1.2 Mesures de protection.

Les mesures générales s'appliquent, quel que soit le contexte dans lequel le poste informatique se situe :

- Prévention des attaques virales,
- Suppression des programmes espions,
- Mise en œuvre d'une stratégie cohérente lors du choix des mots de passe,
- Assurance que le système dispose des dernières mises à jour logicielles,
- Sécurisation des logiciels installés sur la machine,
- Contrôle et blocage des tentatives d'intrusion.

1.2.1 Utilisateurs particuliers

Les mesures de protection, pour un utilisateur particulier, sont simples et consistent à équiper son ordinateur de logiciels (le plus souvent des logiciels gratuits) permettant d'offrir un niveau de sécurité tout à fait correct de sa machine :

- Deux logiciels « antispyware » différents (dont au moins un résident en mémoire).
- Deux antivirus différents.
- Utilisation du pare-feu Windows.
- Scan et nettoyage réguliers du système.
- Mise à jour automatique de Windows (Windows update).
- Clairvoyance dans les téléchargement s et ouvertures de fichiers joint aux courriers mails.

1.2.2 Entreprises et organismes institutionnels

La politique de prévention est mise en œuvre par l'administrateur système et réseau de manière globale, tant au niveau des postes individuels que des serveurs et du réseau.

1.3 Antivirus

Un programme anti-virus est chargé de détecter, d'isoler et de supprimer les fichiers infectés en analysant le contenu de divers supports (disque dur, clef usb, cd-rom, etc …) ainsi que la mémoire vive (ce qu'il fait au démarrage de l'ordinateur).

1.3.1 Désinfection.

La désinfection éventuelle s'opère par :

- Suppression du virus dans le fichier infecté et remise dans son état initial du fichier.
- Suppression éventuelle du fichier infecté ayant pour conséquence l'impossibilité de faire fonctionner parfois certains logiciels.
- Déplacement du fichier infecté en quarantaine (dans une zone du disque dur sécurisée par le logiciel antivirus) en attendant une version capable de le désinfecter. Ce conteneur ne peut être ouvert que par l'antivirus et un double-clic n'activera jamais le programme malveillant.

1.3.2 Composants d'un antivirus

1.3.2.1 Scanner

Le scanner examine (scan) votre ordinateur à la demande : un fichier, un dossier ou tous les fichiers de votre disque. Un scan complet consomme beaucoup de ressources machine et mémoire, mais il est conseillé de le faire de temps en temps.

1.3.2.2 Moniteur

Le moniteur est un programme qui se charge en mémoire de manière résidente, c'est à dire qu'il reste en fonction tant que votre ordinateur est allumé.

C'est un centre de contrôle permanent des activités qui se déroulent sur l'ordinateur ainsi qu'un gestionnaire des fonctions de protection et d'analyse.

Il est chargé d'analyser en permanence (en temps réel) les fichiers auxquels vous accédez (ou qui arrivent par le biais de la messagerie, du Web ou d'un support de données externe) sur votre machine au cours d'une session de travail normale.

Chaque fois qu'un fichier (programme ou autre) doit être chargé en mémoire, le moniteur en examine le contenu, et stoppe l'exécution des instructions de ce fichier si celui-ci comporte des instructions virales.
Il est composé de plusieurs modules dont les fonctions sont spécifiques à chacun des vecteurs possibles d'infection virale :

- E-mail,
- Web,
- Téléchargements,
- Système.

En fonction de sa configuration et de la puissance de votre ordinateur, il ralentit plus ou moins vos applications et votre système

1.3.2.3 Base de signatures de virus

Une signature est une partie de code informatique permettant d'identifier un virus, (une sorte d'empreinte du virus présente dans un fichier contaminé).
La base de signatures référence des dizaines de milliers de virus, troyens et variantes. Elle doit être mise à jour fréquemment pour reconnaître les nouveaux spécimens.

1.3.3 Méthodes de détection virale

Les méthodes changent d'un logiciel à l'autre :

- Les signatures de virus (à mettre à jour souvent : il s'en crée tous les jours)
- L'analyse heuristique recherche un comportement viral dans les programmes, permettant de détecter des programmes malveillants inconnus de la base de signatures. Celle-ci est donc à même de souvent générer de fausses alertes.
- L'examen comportemental surveille la manière dont les logiciels actifs en mémoire accèdent aux fichiers de l'ordinateur et comment ils les manipulent.
- Le contrôle d'intégrité permet de détecter les modifications de fichiers sur le disque, chaque fichier est « marqué » par un identifiant appelé « somme de contrôle » (CRC). Si un virus modifie le fichier, la somme de contrôle change et le logiciel antivirus vous alerte.
- La détection générique multi-niveaux recherche les virus polymorphes.

Malgré toutes ces techniques sophistiquées, il ne faut jamais oublier qu'un antivirus n'est pas efficace à 100 %.

1.3.4 Bloqueur

Un bloqueur empêche l'utilisation des CD, DVD, clefs usb et supprime les pièces jointes des E-mails. Il agit comme un filtre, laissant passer certains fichiers et en arrêtant d'autres.

La diffusion d'un nouveau fichier est contrôlée par l'administrateur qui l'analyse avec un anti-virus (un bloqueur n'est pas un anti-virus).

Dans une politique ultra-sécuritaire, cette défense est insuffisante et trop chère : mieux vaut un parc de machines sans aucun lecteur CD, DVD (ceux des serveurs sont accessibles sous contrôle), supprimer les pièces jointes automatiquement sur le serveur et interdire l'accès à Internet.

1.4 Anti-spyware

Logiciel utilitaire capable de rechercher et d'éliminer les logiciels espions (spywares). Il s'agit le plus souvent d'un scanner à la demande, utilisant une analyse par signatures pour identifier les logiciels espions connus et les désinstaller.

Les méthodes de recherche et de détection varient selon le programme choisi.

1.5 Le pare-feu

1.5.1 Définition – Rôle

Toutes les communications entre votre ordinateur et « l'extérieur » se font par l'intermédiaires de « ports » Ce sont des points d'entrée et de sortie qui permettent d'échanger des informations, dans un sens ou dans un autre, avec une autre machine. Sur Internet, lorsque vous naviguez, vous échangez énormément de données par plusieurs ports différents à plusieurs machines. Il existe en tout et pour tout 65536 (de 0 à 65535) ports sur une machine.

Ainsi, les ports sont indispensables à l'échange d'informations par Internet et constituent les seules entrées existantes vers votre pc, c'est donc par là que les surfeurs malveillants pénètrent dans votre machine. Le pare-feu peut être logiciel ou matériel.

Un pare-feu (appelé aussi firewall) est un système permettant de protéger un ordinateur des intrusions provenant du réseau ou de protéger un réseau local des attaques provenant d'Internet.

Son rôle consiste à contrôler le trafic sur chacun des ports de l'ordinateur, à repérer les connexions suspectes de la machine et également à les empêcher. Il fonctionne donc comme un filtre et s'intercale entre votre ordinateur et l'extérieur.

L'une des techniques de hacking les plus courantes consiste à tester tous les ports d'une machine afin d'en dénicher un laissé ouvert par mégarde.

Les logiciels de scan de port comme « Superscan » testent généralement dans un ordre croissant tous les ports IP. Mais pour que le pare-feu soit réellement imperméable à ce genre de tentative, il doit être correctement paramétré.

De nombreux postes de travail "protégés" sont dans les faits de véritables passoires pour cause de pare feu mal configuré et donc inefficace. Si certains ports doivent rester ouverts pour une utilisation normale d'Internet, il est inutile de laisser les autres ports actifs.

Les ports qui restent ouverts :

Port	Rôle
25	Envoi des messages (SMTP)
110	Réception des messages (POP)
80	Accès à Internet (HTTP)
21	Téléchargement de fichiers (FTP)
119	Forums (NNTP)
6667	Messagerie instantanée (IRC)
53	Serveur de noms (DNS)

Il existe communément 3 états pour un port de votre machine, qui correspondent à trois comportements différents de votre système lorsqu'il reçoit des données sur un port :

- état ouvert (open) : le système accepte le trafic sur le port et une application écoute derrière ce port pour traiter les données reçues. C'est un comportement d'échange ponctuel si le port a été spécialement ouvert pour une occasion précise, ou un comportement serveur s'il demeure ouvert.
- état fermé (closed) : le système renvoit une erreur à l'expéditeur de données sur ce port car aucune application n'est branchée dessus pour traiter les données. C'est l'état le plus courant sur le nombre de ports. Notez qu'envoyer des données sur un tel port permet de savoir que votre ordinateur existe car il répond en renvoyant une erreur.
- état protégé (stealth) : le système ne possède aucune application branchée sur ce port, et ne renvoie pas d'erreur à l'expéditeur de données sur ce port. C'est un comportement particulier dû à un pare feu. Il permet de faire croire qu'aucun ordinateur ne possède l'adresse à laquelle ont été envoyées les données. Personne n'essayera alors de trouver un port ouvert pour s'introduire dans la machine.

Attention toutefois si vous souhaitez bloquer tous les ports de votre machine : certains ports courants sont nécessaires au bon fonctionnement de celle-ci !

1.5.2 Mise en Œuvre d'un pare-feu

De nombreux logiciels de pare-feu sont disponibles par le biais d'Internet, soit en version gratuite (aux fonctionnalités plus réduites mais néanmoins complètes), soit en version payante (offrant alors une étendue de paramétrage plus importante).

Les plus connus sont « Zone Alarm », « Kerio personal Firewall », « Norton Personal Firewall », etc …

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées :
  "Tout ce qui n'est pas explicitement autorisé est interdit".
- Soit d'empêcher les échanges qui ont été explicitement interdits.

Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité choisie.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

A défaut de disposer d'une version de Windows XP (SP2) comportant un pare-feu intégré, il est conseillé d'en télécharger un et de l'installer sur votre machine.

IL NE FAUT JAMAIS INSTALLER 2 PARE-FEU SUR LA MEME MACHINE,
LEURS EFFETS S'ANNULANT ALORS.

2 LES MOTS DE PASSE

2.1 Bien les choisir

De nombreuses attaques informatiques sont directement liées à un mot de passe facilement décodable.

Pour renforcer la sécurité d'un mot de passe et le rendre difficile à découvrir, il doit :

- Se composer d'au moins sept caractères provenant de chacun des trois groupes suivants :

  1 - Lettres (majuscules et minuscules) A, B, C,...; a, b, c,...

  2 - Chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

  3 - Symboles (tous les caractères non définis comme des lettres ou des chiffres) ` ~ ! @ # $ % ^ & * ( ) _ + = { } | [ ] \ : " ; ' < > ? , . /

- Avoir au moins un caractère symbole entre la deuxième à la sixième position,

- Etre totalement différent des mots de passe précédents,

- Ne pas contenir votre nom ou votre nom d'utilisateur, les prénoms des enfants, la date de naissance etc …

- Ne pas être un mot ou un nom commun, même en partie.

Enfin, il convient de rappeler que le principe même d'un mot de passe est de protéger un accès. Évitez donc, comme on le voit trop souvent, d'inscrire celui-ci près de votre ordinateur, sous le clavier, etc …

3 LA MESSAGERIE

3.1 Spamming.

Le « spamming » prend pour cible votre boîte aux lettres mail et désigne l'action d'envoyer un message non souhaité et dérangeant - appelé "spam" - à une personne ou à un groupe de personnes, généralement dans un but promotionnel ou publicitaire.

Il s'agit véritablement d'un usage abusif des fonctionnalités de messagerie en faisant en sorte que les messages reçus soient confondus avec des messages ou des contenus habituellement échangés ou recherchés par les utilisateurs.

Le support utilisé importe peu (courriel, messagerie instantanée, SMS, forum, moteur de recherche, etc.), de même que le nombre de messages envoyés par le spammer.

Le spamming s'accompagne souvent de la part du spammer d'une ou plusieurs pratiques généralement reconnues comme illégales au niveau mondial (usurpation d'identité, collecte déloyale de données personnelles, contrefaçon de marque, escroquerie, entrave volontaire à un système,...).

Si à priori, le spamming n'est pas bien méchant, il devient très vite agaçant par la perte de temps qu'il engendre : publicités pour des produits dont vous n'avez que faire voire pour des sites pornographiques, messages dans une langue incompréhensible... Le téléchargement de mails inutiles augmente le temps de connexion lorsque vous relevez votre courrier, et surtout il faut ensuite passer du temps à trier et éliminer les courriers publicitaires ou parasites, au risque de supprimer un message valable.

3.2 Lutter contre le spamming.

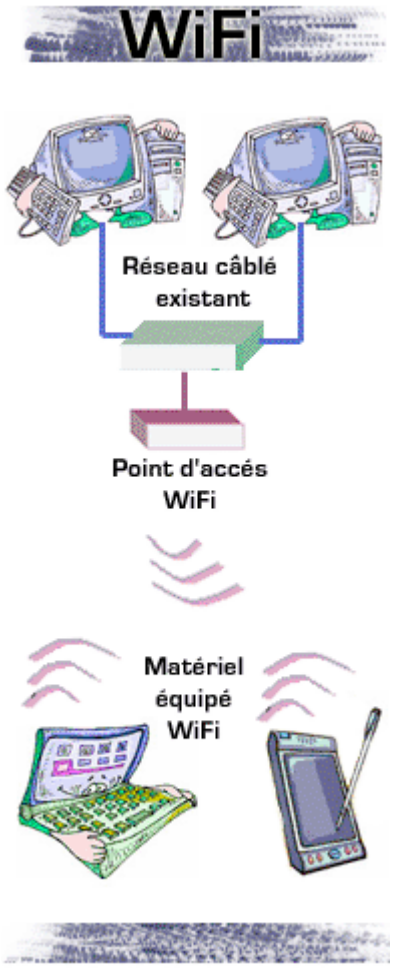
Il est très difficile de stopper la réception de publicités lorsqu'un spammeur a récupéré votre adresse e-mail.
Bien souvent, la situation ne fait qu'empirer au fur et à mesure que l'adresse sera exploitée et revendue à différents intermédiaires et vous contraindra, dans les cas extrêmes, à supprimer purement et simplement votre boîte aux lettres.

Si vous ne souhaitez pas recevoir de publicités non sollicitées (et plus généralement de messages inoportuns) sur une certaine adresse, commencez par choisir un nom d'utilisateur suffisamment long et absent du dictionnaire. Evitez ensuite de publier l'adresse sur Internet, dans votre site ou dans un forum, quitte à utiliser une deuxième adresse pour les situations à risque.

N'hésitez pas à vous créer des adresses que vous n'utiliserez que dans des cas précis (commandes sur Internet, envoi de codes de validation de logiciels, etc…).

4 LE WLAN (WiFi)

4.1 Principe de fonctionnement



Qu'est-ce-que le WiFi?

Le nom Wi-Fi (Wireless Fidelity) correspond initialement au nom donné à la certification délivrée par la WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.

C'est le label et le nom « grand public » pour la plupart des réseaux sans fils qui s'appuient sur les normes 802.11.

Le Wi-Fi permet ainsi de relier plusieurs ordinateurs ou périphériques entre eux, sans fil, par la voie des ondes radio.

Il permet d'échanger et de partager des fichiers, une connexion Internet, des informations, de jouer en réseau, etc...

Les différents types de WiFi :

IEEE 802.11	-	1997	2 Mbps
IEEE 802.11a	802.11A	1999	54 Mbps
IEEE 802.11b	802.11B, Wi-Fi B	1999	11 Mbps
IEEE 802.11g	802.11G, Wi-Fi G	2003	54 Mbps
IEEE 802.11n	802.11N, Wi-Fi N	2009	600 Mbps
IEE 802.11ac	802.11AC, Wi-Fi AC	2014	1.3 Gbps (*)

4.2 Sécuriser son réseau sans fil

Alors que pour s'introduire sur un réseau filaire, il faut s'y relier physiquement, en Wi-Fi, toute personne se trouvant à portée du réseau peut potentiellement s'y raccorder. Et cela est d'autant plus gênant que l'intrus n'est pas forcément visible : cela peut être un voisin, un passant dans la rue, bref, n'importe qui. Libre à lui alors de fouiner sur les disques durs de vos PC reliés au réseau non protégé ou d'utiliser votre connexion Internet à mauvais escient, vous-même étant responsable des actes qu'il pourrait commettre. Il est heureusement possible d'empêcher cela.

Encore faut-il prendre la peine de se plonger dans la configuration de son matériel car, par défaut, les réglages des points d'accès et des routeurs Wi-Fi ne sont pas du tout sécurisés et autorisent quiconque à se connecter à votre réseau. Ainsi, la majorité des utilisateurs qui passent au Wi-Fi, voyant que le réseau sans fil fonctionne dès sa mise en route, ne vont pas plus loin et ne cherchent pas à le sécuriser, ce qui est extrêmement risqué.

4.3 Clefs WEP et WPA/WPA2

4.3.1 Le WEP et ses limites.

Le protocole WEP (Wired Equivalent Privacy ou Protection Equivalente au Câble) utilise une clé d'une longueur de 64 à 256 bits dont 24 ne sont pas utilisés pour le chiffrement. Cela fait une clé, si on la compare à un mot, d'une longueur de 5 à 29 caractères. La majorité des clés est composée de 13 caractères. L'algorithme utilisé dans le chiffrement possède une grande faiblesse qui est exploitée aujourd'hui très facilement par les hackers.

Il suffit de quelques minutes pour reconstituer tous les morceaux de la clé WEP qui circulent de temps à autres sur votre réseau. La raison pour laquelle ils circulent est intimement liée à l'algorithme utilisé car celui-ci doit être initialisé à chaque échange pour ne pas utiliser deux fois la même clé. De fait une partie de la clé (les 24 bits en question) est utilisée comme élément d'initialisation (vecteur d'initialisation) et celui-ci n'est pas chiffré.

Au bout d'un moment, si quelqu'un écoute tous les échanges, il aura obtenu suffisamment d'éléments pour reconstruire la clé sans la connaître au préalable. Pour cette raison la clé WEP ne doit absolument plus être utilisée sur les équipements Wi-Fi aujourd'hui.

4.3.2 Le WPA / WPA2

Le protocole WPA offre une protection d'un niveau bien supérieur à WEP. Il utilise pourtant le même algorithme de chiffrement et est basé sur le même principe de vecteur d'initialisation. En revanche le TKIP (Temporal Key Integrity Protocol ou Protocole d'intégrité par clé temporelle) a été ajouté, permettant ainsi une permutation plus importante des clés sans que le vecteur d'initialisation ne puisse être reconstitué de manière utile.

Dans les configurations les plus courantes, le mode Personnel est utilisé avec la PSK (Pre-Shared Key ou clé pré-partagée). Cela permet d'utiliser une clé alphanumérique normale d'une longueur d'au moins 32 caractères. Ce qui offre un niveau de protection tout à fait acceptable.

Le protocole WPA2 quant à lui utilise un algorithme de chiffrement beaucoup plus puissant, utilisé dans le cryptage des documents sensibles et possédant une clé très forte. Il s'agit de la dernière norme du protocole WPA permettant de protéger votre réseau WLAN.

Il est conseillé d'indiquer une clé assez longue, d'un minimum de 20 caractères, pour assurer une certaine efficacité quant à la sécurisation du réseau.

5 LES TRANSACTIONS PAR INTERNET

5.1 Principes de sécurisation des transactions

Il est paradoxal de constater que nombre d'utilisateurs sont peu enclins à communiquer leur numéro de carte bancaire sur un site web, alors qu'ils le font régulièrement lorsqu'ils règlent l'addition au restaurant ou qu'ils payent leurs achats dans leur supermarché ou leur magasin favori.

C'est pourquoi la majorité des sites de commerce électronique mettent en avant que les transactions effectuées via leurs serveurs sont "sécurisées" et que les clients potentiels peuvent donc acheter sans crainte.

Certains sites vont même jusqu'à adhérer à des organisations professionnelles délivrant un label prouvant qu'il n'y a aucun risque à effectuer des transactions sur leur site internet. D'autres proposent des indemnités financières en cas d'utilisation frauduleuse du numéro de carte qui aurait été obtenu par un individu malveillant lors d'un achat sur le site en question.

5.2 Les sites sécurisés.

5.2.1 Sans intermédiaire financier.

Les sites marchands sans intermédiaire financier traitent directement les numéros de cartes des clients et les conservent, pour une durée généralement non précisée, au sein de leurs bases de données.

Ces sites sont vulnérables à des attaques et doivent donc se protéger en conséquence.

Sur un plan purement sécuritaire, il serait préférable que ces sites ne conservent les numéros de carte de leurs clients que pour la durée nécessaire au traitement de leur commande, soit de quelques jours à quelques semaines, grand maximum.

Malheureusement, dans un souci de faciliter la vie des acheteurs réguliers, nombres de sites conservent les numéros de cartes de leurs clients, de façon à leur éviter la fastidieuse saisie des 15 ou 16 chiffres les composant.

Le recours à un intermédiaire financier ayant par ailleurs un certain coût, nombre de petites structures de ventes ne font pas appel a eux et traitent donc directement les commandes des clients.

5.3 Avec intermédiaire financier

Ces sites font appel aux services de sociétés tierces qui assurent, lors de la phase de paiement par l'acheteur, la redirection de son navigateur sur le site d'une grande banque ou d'un intermédiaire financier.

Ce dernier demande la saisie du numéro de carte et de la date de validité associée ainsi que du cryptogramme figurant au dos de la carte.

Généralement, après vérification auprès de l'organisme ayant délivré la carte (via le Réseau Carte Bancaire), l'intermédiaire renvoie un code de retour positif au site marchand, lui indiquant que le paiement s'est effectué correctement.

Ainsi, la commande peut être expédiée au client.

L'avantage de ce type d'intermédiaire est qu'il ne conserve le plus souvent les numéros de cartes bancaires qu'il reçoit que pendant le temps nécessaire à leur traitement. De plus, le commerçant n'a jamais connaissance du numéro en question, donc s'il est malhonnête, il ne pourra pas débiter votre compte à sa guise. Enfin, il est plus facile de sécuriser un serveur spécialisé dans le paiement par carte que toute l'infrastructure mise en place dans le cas d'un site d'e-commerce traitant lui-même les dits numéros.

5.4 Le protocole SSL.

Pour sécuriser les informations, on utilise un protocole nommé SSL (Secure Sockets Layer) afin de "sécuriser" les paiements.

Ce protocole a été inventé par Netscape et est devenu standard Internet par la suite.

On reconnaît aisément son utilisation par la présence d'un petit symbole dans la barre de statut des navigateurs web (cadenas ou clé) et par le préfixe "https://" en tête des URL affichées dans la barre d'adresses de ces navigateurs.

Aucune transaction ne doit être envisagée sur un site non sécurisé (dont l'adresse ne commence pas par https://).

Ce protocole à deux finalités :

- Authentifier le serveur sur lequel vous voulez faire des achats.
- Assurer la sécurisation des données que vous allez transmettre pour effectuer votre achat.

5.4.1 Authentification du serveur.

Cette opération est réalisée à l'aide de ce qu'on appelle un certificat numérique, sans lequel le protocole SSL ne peut fonctionner. Ce certificat est délivré par des sociétés, appelées opérateurs ou autorités de certification, qui délivrent des cartes d'identité

numériques valables généralement un an et attestant que le serveur X appartient bien à la société X, garantissant que lorsque vous vous connectez sur le site d'un vendeur, vous êtes bien sur son site et pas sur celui d'un autre.

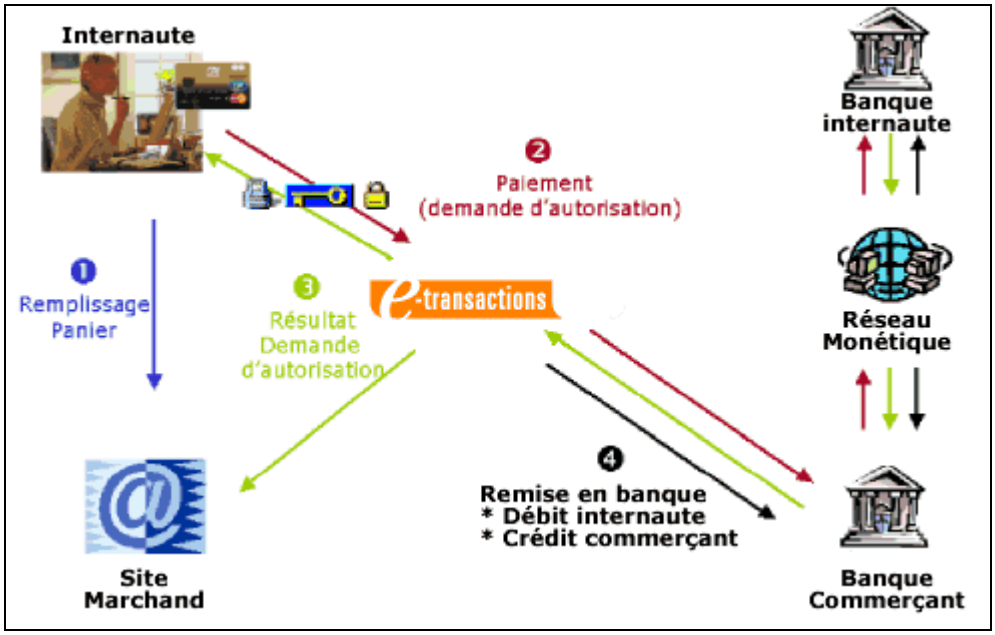
5.4.2 Confidentialité des informations transmises.

Pour ce faire, les informations transmises vont être cryptées grâce à l'utilisation d'algorithmes de chiffrement.
La "force" de ces algorithmes est déterminée par la longueur de clé utilisée pour effectuer ce chiffrement, exprimée en bits.
Le choix de l'algorithme de chiffrement ainsi que la longueur de la clé utilisée font l'objet d'une négociation, lors de l'ouverture d'une session SSL, entre le client (navigateur) et le serveur (site d'e-commerce). Cette négociation repose sur les capacités et les caractéristiques des logiciels employés de part et d'autre.

La question qui se pose est de savoir si l'on peut réellement transmettre sans risque un numéro de carte bancaire via Internet. En fait, la réponse est oui. Bien qu'il soit techniquement et théoriquement possible de récupérer puis de décrypter les informations transmises, en pratique, aucun pirate ou hacker ne se donnera la peine d'intercepter un flux SSL chiffré, afin de tenter d'en extraire votre numéro de carte bancaire

Il est bien plus rentable, et parfois bien plus facile, de s'attaquer directement au site du commerçant afin de lui soutirer les milliers de numéros valides qu'il a pu stocker dans ses bases de données.

SCHEMA RECAPITULATIF D'UNE TRANSACTION



6 LE PEER TO PEER – TELECHARGEMENT.

6.1 Définition

Le peer-to-peer est un réseau d'échange et de partage de fichiers entre internautes.

Il existe un grand nombre de réseaux « peer-to-peer » (KaZaA, Gnutella, Emule, etc.) avec chacun ses points forts et points faibles (sécurité, anonymat, vitesse de téléchargement, vidéos, musique, logiciels).

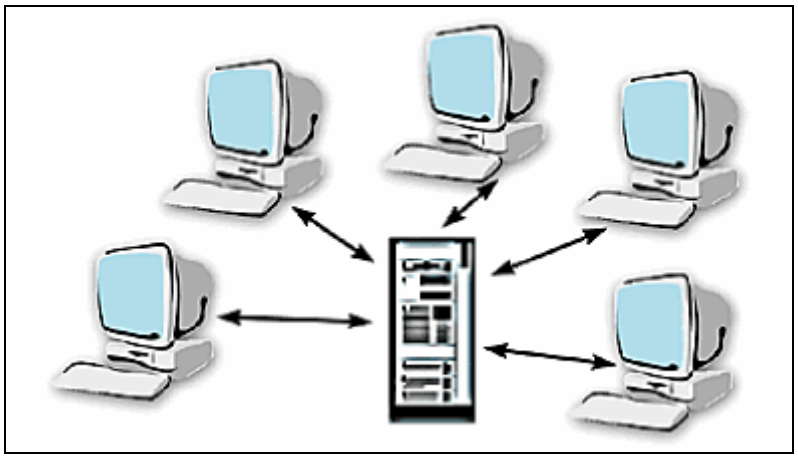
6.2 Description

Le principe du « peer-to-peer » (P2P) est de mettre directement en liaison un internaute avec un autre internaute qui possède un fichier convoité.

Le P2P est utilisé en grande partie pour télécharger des fichiers piratés (logiciels, DVD, musique). Il fait l'objet d'attaques répétées des industriels qui produisent ces oeuvres. Les réseaux décentralisés sont difficilement attaquables en justice, les industriels centrent leur action sur les internautes qui utilisent les réseaux P2P et les fournisseurs d'accès à Internet.

Il existe 2 méthodes pour assurer la liaison entre les ordinateurs désireux d'accomplir des échanges P2P.

6.2.1 Méthode centralisée

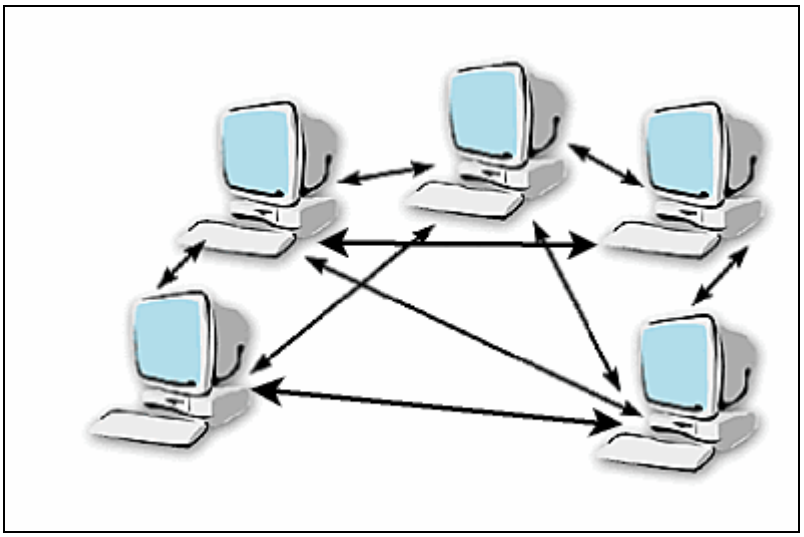


Un serveur central possède la liste des fichiers disponibles sur les ordinateurs des internautes connectés à ce serveur central. Il sait donc où se trouvent tous les fichiers disponibles et mis à la disposition de tous ceux qui sont connectés à un instant donné.
Lorsqu'un internaute fait une recherche pour trouver un fichier, le serveur central le dirige vers l'ordinateur de celui qui le possède et le téléchargement peut ainsi avoir lieu directement entre un utilisateur et un autre.

C'est ainsi que fonctionnait « Napster » avant son démantèlement par décision judiciaire.
Kazaa utilise cette technologie.

L'un des principaux avantages de ce modèle est l'index central qui permet de localiser les fichiers rapidement et efficacement, grâce à la base de donnée régulièrement mise à jour du serveur. Par ailleurs, dans cette configuration, tous les clients sont obligés d'être connectés sur le réseau du serveur : la requête atteint donc tous les utilisateurs connectés, ce qui rend la recherche encore plus pertinente.
Principal inconvénient : en cas de panne du serveur central, plus aucune recherche ni téléchargement ne sont possibles.

6.2.2 La méthode décentralisée.



Dans ce cas, il n'y a pas de serveur central.

Au lancement du programme de « «peer-to-peer », l'ordinateur de l'internaute se « transforme » en serveur, et tous ces « mini serveurs » se trouvent reliés entre eux par le biais du logiciel de « peer-to-peer » qui fonctionne sur toutes les machines. Le tout constitue alors un réseau de serveurs individuels.
Par ce biais, chacun des utilisateurs met à disposition de l'ensemble de la communauté une certaine partie des fichiers de son ordinateur pour téléchargement.

Lorsqu'un utilisateur cherche un fichier, sa demande est transmise à la communauté des utilisateurs et est communiquée à l'ensemble des machines du réseau, ce qui génère un trafic énorme sur Internet, et ralentit, de surcroît, considérablement le processus de recherche puisqu'il n'y a pas de serveur central pour indiquer directement à quelle ordinateur se connecter pour trouver le fichier demandé.

Cette méthode a l'avantage de répartir les responsabilités et d'éviter les actions en justice.

C'est sur ce modèle que fonctionnent, par exemple, Gnutella et Emule

6.3 Les dangers

Les applications dédiées à ce mode de transfert permettent le partage de fichiers sans réel contrôle. Votre machine se comportant comme un serveur peut héberger des fichiers à votre insu, voire des logiciels qui ouvrent ainsi la porte à des hackers (pirates).

Le contenu des fichiers téléchargés peut ne pas être en rapport avec le nom qu'ils affichent et avoir des effets biens différents de ce que l'on attend.

De très nombreux fichiers contenant des virus sont propagés sur le réseau par ce biais.

La législation visant à réduire le piratage d'œuvres musicales a été considérablement renforcée. Votre responsabilité est pénalement engagée. Les sanctions sont souvent très lourdes : amendes et prison.

L'utilisation de logiciel de « peer-to-peer » est, bien sûr, totalement déconseillée dans le cadre d'un environnement professionnel…

7 Le piratage.

7.1 La définition de « logiciel ».

Selon l'arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire informatique, le logiciel est défini comme "l'ensemble des programmes, et éventuellement la documentation, relatifs au fonctionnement d'un ensemble de traitements de l'information".

Le Code de la Propriété Intellectuelle précise que cette définition comprend "le matériel de conception préparatoire" (article L.112-2), précisé comme étant "les travaux préparatoires de conception aboutissant au développement d'un programme, à condition qu'ils soient de nature à permettre la réalisation d'un programme d'ordinateur à un stade ultérieur".

Cette définition inclut donc le dossier d'analyse et schémas décrivant les traitements à effectuer.

7.2 Risques encourus.

Le logiciel est une œuvre de l'esprit. Il bénéficie à ce titre de la protection des droits d'auteur définie par le Code de la Propriété Intellectuelle (CPI).
La loi dispose que toute représentation ou reproduction intégrale ou partielle d'un logiciel faite sans le consentement de son auteur est illicite et qualifie de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel.

L'exception pour copie privée n'existe pas pour le logiciel. Seule une copie de sauvegarde est permise si la copie originale est détruite.

Le Code de la Propriété Intellectuelle stipule :
Article L.335-3 "Est (...) un délit de contrefaçon la violation de l'un des droits de l'auteur de logiciel (...)."
Article L.122-4 "Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur (...) est illicite."
Article L.335-2 "La contrefaçon en France (...) est punie de deux ans d'emprisonnement et de **150.000 Euros d'amende**." Comme le stipule l'article 131-38 du Nouveau Code Pénal, *ce montant peut être multiplié par cinq dans le cas d'une personne morale et donc* ***atteindre 750.000 Euros d'amende.***

Le piratage de logiciels peut donc se définir comme étant toute infraction aux lois régissant les droits de la propriété intellectuelle (droits d'auteur) et la protection juridique des programmes d'ordinateur.

7.3 Les parades de Microsoft.

Pour télécharger des logiciels Microsoft ou des mises à jour, il FAUT être en règle.

Concrètement, l'accès au site de téléchargement de Windows est réservé aux internautes possédant une licence originale de leur système d'exploitation.

Ils doivent souscrire au programme *Windows Genuine Advantage* (WGA), ce qui pourrait se traduire par « l'avantage d'avoir un Windows authentique ».

Pour être membre de WGA, il suffit de se soumettre à une simple vérification en ligne de la conformité de sa copie de Windows XP ou 2000. En échange, les internautes ont droit à quelques bonus : des logiciels commerciaux (Photo Story et Winter Fun 2004) en téléchargement gratuit, ainsi que des remises sur des jeux en ligne et sur des services.

Cependant, copie licite ou non, les mises à jour de sécurité critiques restent libres d'accès par le biais de Windows Auto Update.

8 CONSERVER SES DONNEES.

Une précaution élémentaire consiste à dupliquer les données essentielles en les sauvegardant sur plusieurs supports différents, rangés en lieu sûr.

Il reste toujours possible, en cas de problème (panne de disque dur, attaque virale) de réinstaller le système d'exploitation et les logiciels à partir de CD d'origine.

En ce qui concerne les données propres à chaque utilisateur, tout ce qui n'a pas été préalablement sauvegardé sur un autre support est bien souvent définitivement perdu…

Faites donc régulièrement des sauvegardes en utilisant un support approprié au volume et à la nature des données à conserver.

8.1 Les supports de stockage.

8.1.1 Clefs USB.

La sauvegarde des fichiers se fait dans des modules de « mémoire flash » à l'intérieur de la clef USB. Il s'agit de composants électroniques qui conservent les informations enregistrées sans les perdre lorsque le courant est coupé. Outre les clefs USB, on retrouve ces composants de « mémoires flash » dans les cartes mémoire pour appareils photo numériques, téléphones portables, etc…

Avec les mémoires flash, la consommation électrique est très faible (ce qui permet de les alimenter par le port USB). De plus, le temps d'accès à l'information est très rapide parce qu'il n'y a plus aucun mouvement mécanique. L'information est donc directement accessible.

Les clefs USB et les supports de stockage utilisant de la « mémoire flash » ont cependant quelques inconvénients :

- Le prix de la « mémoire flash » est encore supérieur à celui du support magnétique.
- Le temps d'écriture des informations est encore lent du fait de la technologie employée.
- La capacité de stockage, bien qu'étant en constante augmentation, ne peut rivaliser avec un disque dur externe par exemple.

Elles sont peu adaptées à une politique de conservation de données dans le temps. On préfèrera, dans ce cas, la gravure de CD ou de DVD.

8.1.2 Gravure CD/DVD.

Les graveurs de CD/DVD sont maintenant présents sur la quasi-totalité des ordinateurs du marché (sauf les ordinateurs portables les plus récents).

Les CD/DVD offrent de grandes capacités de stockage et sont donc particulièrement bien adaptés à la sauvegarde et à l'archivage de données. Il n'est pas inutile de rappeler ici que ces supports doivent être rangés en lieu sûr et restent très sensibles aux manipulations diverses (rayures).

Type de support	Capacités de stockage
CD-R / CD RW	700 Mo de données Inadapté au stockage vidéo
DVD-ROM simple face – simple couche Une seule face, une seule couche de données sur cette face.	4,7 Go de données ou 130 minutes de vidéo
DVD-ROM simple face – double couche. Sur une même face, deux couches de données sont superposées, comme si l'on avait deux disques l'un sur l'autre.	8,5 Go de données ou 240 minutes de vidéo
DVD-ROM double face – simple couche. Les données peuvent être lues/écrites sur les deux faces, comme si l'on avait deux cd/DVD collés dos à dos.	9,4 Go de données ou 260 minutes de vidéo
DVD-ROM double face – double couche. Comme si l'on avait deux DVD simple face - double couche collés dos à dos	17,0 Go de données ou 480 minutes de vidéo

Quel que soit le type du CD ou du DVD, il n'y a pas de réelle différence physique visible. Seule la structure interne change.

8.1.3 Disque Externe.

Le disque dur externe permet de stocker vos données de manière fiable. Cependant, pour des opérations d'archivage pur, la gravure de CD/DVD est préférable.

8.1.4 Hébergement sur serveur web (Cloud).

Certains sites Internet proposent de sauvegarder vos données sur leurs serveurs. Ces services sont généralement payants et s'adressent plus à des entreprises qu'à des particuliers en regard du coût annuel de l'hébergement.

Néanmoins, il sera souvent possible d'utiliser l'espace disque mis à votre disposition par l'hébergeur de votre site Internet (si vous en avez un) pour y stocker des fichiers de données que vous souhaitez sauvegarder.

Vous pourrez aussi vous servir de votre compte de messagerie (si les fichiers ne sont pas trop volumineux et que la boite mail accepte le type de fichier envisagé) pour réaliser ce type de sauvegarde. Cependant, cette méthode ne saurait être envisagée comme étant le moyen principal de sauvegarde de vos données (risque de suppression de compte, de messages, etc…).

8.2 L'archivage de données.

Il sera réalisé, soit par simple copie de fichiers à partir de l'explorateur de Windows, soit pas compression (logiciel d'archivage) et copie des archives, soit en utilisant des programmes spécifiques d'archivage de données (certains, tel « ULTRABACKUP » sont disponibles gratuitement sur Internet).

Ne multipliez pas inutilement les copies des données. Vous risqueriez de ne plus « vous y retrouver » entre les différentes versions de vos fichier et d'obtenir finalement, un résultat contraire au but recherché.

Un solution raisonnable consiste donc à utiliser un logiciel de sauvegarde dont vous aurez programmé l'exécution à intervalles réguliers (à déterminer selon la nature et la fréquence de vos travaux sur vos fichiers – une période de 15 jours entre deux sauvegardes semble être un maximum).

8.3 Restauration en cas de problème.

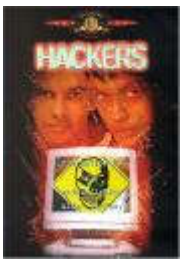
En fonction de la nature des problèmes rencontrés, les modes de restauration vont varier de la simple copie de fichier effacé par mégarde à la réinstallation complète du système d'exploitation, des logiciels et des données.

Quoiqu'il en soit :

- Conservez précieusement les CD/DVD d'origine de tous vos logiciels (faîtes-en éventuellement des copies de sauvegarde), ainsi que les numéros de licence correspondant.
- Conservez en lieu sûr des copies de vos données les plus importantes en prenant soin de bien actualiser ces copies.

9 HACKERS ET CRACKERS.

9.1 Qu'est-ce qu'un hacker ?



Le terme «**hacker**» est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatiques aiment à penser qu'ils ont été attaqués par des pirates chevronnés ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour en exploiter les failles.

Le terme *hacker* a eu plus d'une signification depuis son apparition à la fin des années 50. A l'origine ce nom désignait des programmeurs émérites, puis il servit au cours des années 70 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques.
C'est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.

Aujourd'hui, ce mot est souvent utilisé, à tort, pour désigner les personnes s'introduisant dans les systèmes informatiques.

9.2 Les buts du hacker

Le propos n'est pas ici d'entamer une polémique sur les motivations des hackers mais simplement de mieux comprendre la manière dont ils agissent.

Les hackers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des **failles**, c'est-à-dire des *vulnérabilités* nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation ! Les termes de **vulnérabilité**, de **brèche** ou en langage plus familier de **trou de sécurité** (en anglais *security hole*) sont également utilisés pour désigner les failles de sécurité.

Pour pouvoir mettre en œuvre un exploit (il s'agit du terme technique signifiant *exploiter une vulnérabilité*), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci. La plupart des attaques sont l'oeuvre de *script kiddies* essayant bêtement des exploits trouvés sur Internet, sans aucune connaissance du système, ni des risques liés à leur acte.

Une fois que le hacker a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.

Lorsqu'un accès administrateur (le terme anglais *root* est généralement utilisé) est obtenu, on parle alors de compromission de la machine (ou plus exactement en anglais *root compromise*), car les fichiers systèmes sont susceptibles d'avoir été modifiés. Le hacker possède alors le plus haut niveau de droit sur la machine.

La dernière étape du hacker consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

9.3 Les différents types de hackers.

En réalité il existe de nombreux types d'"*attaquants*" catégorisés selon leur expérience et selon leurs motivations.

9.3.1 Les white hat hackers,

Ce sont les hackers au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques. Ils sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui. Le courrier électronique en est un exemple.

Leur but est simplement de rechercher d'éventuelles failles dans les systèmes informatique afin de les améliorer et de les sécuriser d'avantage.

9.3.2 Les black hat hackers,

Plus couramment appelés *pirates* (ou appelés également *crackers* par extension du terme), c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans un but nuisible.

9.3.3 Les Script Kiddies

Peut être traduit par « *gamins du script »*, parfois également surnommés *crashers*, *lamers* ou encore *packet monkeys*, soit *les singes des paquets réseau*. Ce sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.

9.3.4 Les phreakers

Ce sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques (qualifiées de *box*, comme la *blue box*, la *violet box*, ...) connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement. On appelle ainsi «**phreaking**» le piratage de ligne téléphonique.

9.3.5 Les carders

Pirates qui s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles.
Le terme **carding** désigne le piratage de cartes à puce.

9.3.6 Les crackers

Sont des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants en vue de les utiliser sans les payer. Un «crack" est ainsi un programme créé exécutable chargé de modifier (*patcher*) le logiciel original afin d'en supprimer les protections.

9.3.7 Les hacktivistes

Peut se traduire par « *cybermilitant »* ou « *cyberrésistant »* (contraction de *hackers* et *activistes).*
Ce sont des hackers dont la motivation est principalement idéologique. Ils mettent généralement leurs « talents » au service de leurs convictions politiques en organisant des opérations coup de poing technologiques : piratages, détournements de serveurs, remplacement de page d'accueil de site Internet par des tracts...

9.3.8 Conclusion

Dans la réalité, ce type de distinction est très loin d'être aussi nette, dans la mesure où certains (white hat) hackers ont parfois été crackers (black hat hackers) auparavant et parfois inversement. Les habitués des listes de diffusion et des forums voient souvent des sujets à propos de la différence qu'il convient de faire entre *pirate* et *hacker*. Le terme de *troll* est généralement utilisé pour désigner les sujets délicats déclenchant un engouement dans les réponses.

9.4 Terminologie underground.

Voici un certain nombre de définitions propres au milieu "underground" :

Warez	Piratage de logiciels.
Appz	Piratage d'applications. (contraction de *applications* et *warez*).
Gamez	Piratage de jeux vidéos. (contraction de *games* et *warez*).
Serialz	Piratage de numéros de série permettant d'enregistrer illégalement des copies de logiciels commerciaux. (contraction de *serials* et *warez*).
Crackz	Programmes écrits par des *crackers*, destinés à supprimer de manière automatique les systèmes de protection contre la copie des applications commerciales. (contraction de *cracks* et *warez*).

10 MAC ET SECURITE.

Contrairement aux croyances populaires, le système d'exploitation des ordinateurs Macintosh n'est pas à l'abri des codes malveillants et des attaques de pirates informatiques.

De nombreuses vulnérabilités et failles ont été ainsi détectées et certains programmes malveillants (tels Opener) ciblaient les ordinateurs équipés de Mac OS X.

La croissance des parts de marché de l'OS d'Apple attire l'attention sur ses vulnérabilités et sur leur exploitation.

Il semble évident que plus la popularité des plates-formes d'Apple sera forte, plus le nombre de failles et d'attaques sera élevé.

A l'heure actuelle, le système d'Apple qui ne représente qu'une faible proportion de machines connectées, intéresse peu les hackers.

Les virus Macintosh sont spécifiques au Mac et ne peuvent infecter des programmes Windows.

11 DEJOUER LES PIEGES… UN EXEMPLE

11.1Le but recherché.

De nombreux internautes se sentent pousser des ailes de pirates…
Certains rêvent de pouvoir obtenir, par exemple, par des moyens frauduleux, un mot de passe correspondant à compte MSN qui n'est pas le leur…
Une rapide recherche sur Internet fournit un certain nombre de « méthodes » qualifiées d'infaillibles par les auteurs de ces pseudo techniques.

11.2Comment ?.

Le principe est simple : on vous demande de faire parvenir un E-mail à une adresse (un compte de messagerie le plus souvent) en fournissant, impérativement :

- Votre propre identifiant Facebook.
- Votre mot de passe.
- Le nom du compte dont vous souhaitez obtenir le mot de passe.

On vous demande de patienter quelques heures (et pour cause…) et vous devriez, comme par miracle, obtenir le mot de passe de la personne dont vous souhaitez pirater le compte. C'est magique !!!

Et on vous assure, pour rendre le tout un peu crédible, que « j'ai testé cette solution et ça marche »… Ben voyons…

Ces informations seront « diluées » dans un message comportant (selon l'imagination de l'auteur) des suites de chiffres, du texte sibyllin, ou tout autre élément au choix.

11.3Le résultat…

Le piège est tellement grossier que l'on peut se demander comment certaines et certains peuvent tomber dedans !!!

11.4Les dégâts :

Un individu peu scrupuleux créé un compte de messagerie en lui donnant un apparence un peu technique ou plus ou moins officielle : retrieve_password@hotmail.fr , recup_mdp@hotmail.fr, ou tout autre chose du même genre.

Vous lui adressez **VOTRE ADRESSE ET VOTRE MOT DE PASSE**.
L'adresse de celui ou celle que vous désirez pirater n'a finalement aucune importance.
Le texte dans lequel ces informations sont diluées non plus.

Et vous venez de fournir, tous les éléments pour que votre propre compte Facebook soit piraté…

N'attendez rien en retour, si ce n'est d'éventuels « dégâts » (récupération de vos contacts, envoi de messages diffamatoires, etc.…) sur votre propre compte, que vous ne constaterez que bien tardivement dans la plupart des cas…

11.5En conclusion :

Si une méthode infaillible existait pour pirater un compte Facebook, on peut raisonnablement penser que les développeurs en charge de la gestion de Facebook, y auraient sans doute déjà pensé.

Le travail de ces mêmes programmeurs consiste aussi à tenter de forcer les comptes par des méthodes diverses et variées (et bien plus sophistiquées que celle présentée ci-dessus) afin de sécuriser leurs programmes et appliquer les parades nécessaires lorsqu'ils découvrent une possibilité de piratage.

De plus, il semble évident que l'information ne mettrait que quelques minutes pour remonter à la source, entraînant immédiatement une réponse appropriée sous forme de correctif.

Pirates amateurs, pirates éventuels, pirates de tout poil, ne rêvez pas …

12 Mémo rappel …

Ne désactivez jamais la protection antivirus et vérifiez régulièrement sa validité.
N'ouvrez jamais de pièce jointe aux messages du courrier électronique.
Sauvegardez les pièces jointes et testez les avec l'antivirus installé sur votre machine avant de les ouvrir.
Considérez tout fichier exécutable reçu en tant que pièce jointe comme potentiellement dangereux.
Laissez toujours active la demande de confirmation d'activation des macros de Word et Excel
Faites les mise à jour « windows Update » régulièrement ou planifiez les pour une réalisation automatique.
Ne faites jamais suivre les chaînes.
Méfiez-vous des téléchargements : Beaucoup de site de téléchargement ne vous permettent pas de simplement télécharger un fichier mais vous demandent de télécharger d'abord un téléchargeur (Downloader) qui va, prétendument, mieux gérer le téléchargement. Il s'agit systématiquement d'un cheval de Troie. Recherchez une autre source pour copier votre fichier et évitez ce type de site.
Faites des sauvegardes régulières de vos fichiers de données et de vos applications en utilisant, si nécessaire un logiciel de sauvegarde automatisée.
« Nettoyez » régulièrement votre ordinateur au moyens d'outils tels que CCleaner et ADwCleaner.
Réinitialiser régulièrement votre navigateur avec ses paramètres par défaut et désactivez toutes les extensions inutiles.