

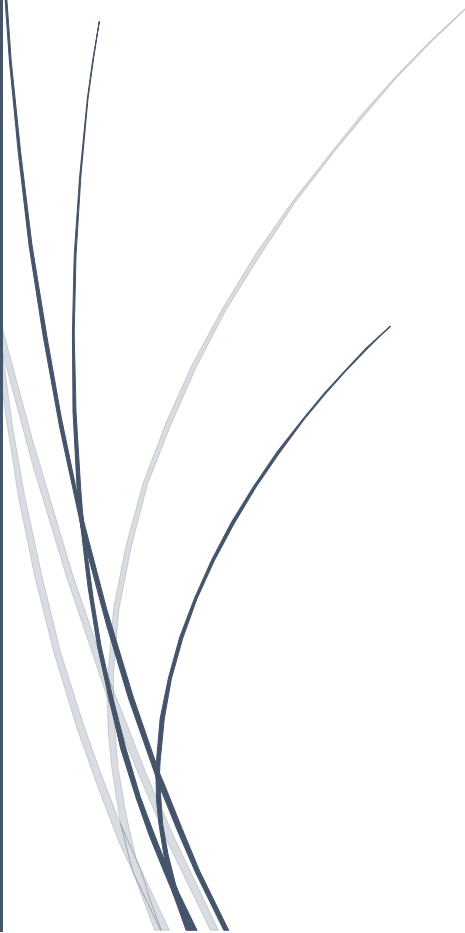
A dark blue vertical bar on the left side of the page. A blue arrow points to the right from the bar, containing the text '2015/2016'.

2015/2016

Notes de cours

Module : Sécurité Informatique

EDITION N°1

Several thin, curved lines in dark blue and light grey originate from the bottom left corner and sweep upwards and to the right.

Enseignant : Samir BOULDJADJ
UNIVERSITE FERHAT ABBAS- SETIF 1



Table des matières

Chapitre 1 – Introduction à la sécurité informatique	1
1. Terminologie :.....	1
2. Menaces possibles.....	2
Chapitre 2 – Techniques cryptographiques classiques	4
1. Modèle de chiffrement conventionnel	4
2. Techniques cryptographiques classiques	4
2.1 Chiffrement monoalphabétique	4
2.1.1 Substitution arbitraire.....	5
2.1.2 Chiffre de Playfair	5
2.2 Chiffres à substitution polyalphabétique.....	6
2.2.1 Le chiffre de Vigenère.....	6
2.3 Chiffres à transposition.....	7
2.3.1 Masque Jetable	7
Chapitre 3 – Les attaques.....	8
1. Qu'est-ce que c'est ?	8
2. Le but du hacking	8
3. Les types d'attaques.....	8
3.1 Les attaques directes	9
3.2 Les attaques indirectes par rebond	9
3.3 Les attaques indirectes par réponse.....	9
4. Exemples des Attaques	9
4.1 L'attaque Boink	9
4.2 Le Mail Bombing.....	9
4.3 IP spoofing.....	10
4.4 DNS spoofing	11
4.4.1 Description de l'attaque DNS ID Spoofing.....	11
4.4.2 DNS Cache Poisoning.....	11
4.5 Déni de service	12
4.6 Web bug	12
4.7 Les Virus	12
4.7.1 Virus réticulaire (botnet)	13
4.7.2 Les Vers.....	13

Sommaire

4.7.3	Cheval de Troie.....	13
4.7.4	Porte dérobée	13
4.7.5	Bombe logique	13
4.7.6	Logiciel espion.....	14
4.8	Logiciel de sécurité non autorisé.....	14
4.9	Courrier électronique non sollicité (spam)	14
4.10	Social engineering.....	15
5.	Protections.....	15
5.1	FORMATION DES UTILISATEURS.....	15
5.2	POSTE DE TRAVAIL.....	15
5.2.1	LES ANTIVIRUS	15
5.2.2	Méthodes d'éradication du Virus	17
6.	Conclusion	17

Important : ces notes de cours s'accompagnent d'un cours ex-cathedra. Ceci explique pourquoi certains passages peuvent paraître succincts, elles ne devraient pas remplacer vos notes de cours.

Chapitre 1 — Introduction à la sécurité informatique

La prolifération des ordinateurs et des systèmes de communication dans les années 1960 à amener le secteur privé à protéger l'information sous forme numérique et à fournir des services sécurisés. La sécurité des données est entièrement dépendante de deux choses :

- la force de l'algorithme cryptographique
- le secret de la clé

La cryptologie est la science des messages secrets. Longtemps restreinte aux usages diplomatiques et militaires, elle est maintenant une discipline scientifique à part entière, dont l'objet est l'étude des méthodes permettant d'assurer les services d'intégrité, d'authenticité et de confidentialité dans les systèmes d'information et de communication :

- l'intégrité des données : un service d'intégrité garantit que le contenu d'une communication ou d'un fichier n'a pas été modifié par des personnes non autorisées ou inconnues.
- Un service d'authenticité garantit l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier. Lorsqu'il s'agit d'un fichier et que l'entité qui l'a créé est la seule à avoir pu apporter la garantie d'authenticité, on parle de non-répudiation. Le service de non-répudiation est réalisé par une signature numérique.
- Un service de confidentialité garantit que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers. Des services de confidentialité sont offerts dans de nombreux contextes (en téléphonie mobile, en télévision à péage,...)

La cryptologie se partage en deux sous-disciplines, également importantes : la cryptographie dont l'objet est de proposer des méthodes pour assurer les services définis plus haut, et la cryptanalyse qui recherche des failles dans les mécanismes ainsi proposés.

1. Terminologie :

- **Intimité et confidentialité** : Garder les informations secrètes de tous sauf les personnes autorisées à les voir.
- **Intégrité des informations** : Assurer que les informations n'ont pas été altérées par des personnes non autorisées ou inconnues.
- **Authentification ou identification d'entité** : La confirmation de l'identité d'une entité.
- **Message d'authentification** : La confirmation de la source de l'information.
- **Signature** : Les moyens de lier l'information à une entité.
- **Autorisation** : Le transfert de la sanction officielle à une autre entité, à faire ou être quelque chose.
- **Validation** : Les moyens de fournir l'autorisation d'utiliser ou de manipuler des informations.
- **Contrôle d'accès** : Limiter l'accès des ressources aux personnes privilégiées.
- **Certification** : L'approbation de l'information par une entité de confiance.
- **Inclusion du temps** : L'enregistrement du temps de création et d'existence de l'information.

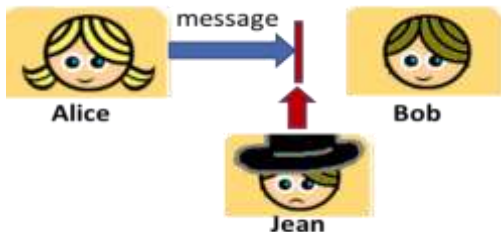
- **Vérification des témoins** : La vérification de la création ou de l'existence de l'information par une entité autre que son créateur.
- **Réception** : Approuver la réception de l'information.
- **Confirmation** : Approuver que le service ait été fourni.
- **Propriété** : Les moyens de fournir à une entité le droit d'utiliser ou de transférer une ressource à d'autres.
- **Anonymat** : Cacher l'identité d'une entité impliquée dans un processus.
- **Non-répudiation** : Empêcher le démenti d'engagements ou d'actions précédentes.
- **Révocation** : La rétraction d'une certification ou d'une autorisation.

2. Menaces possibles

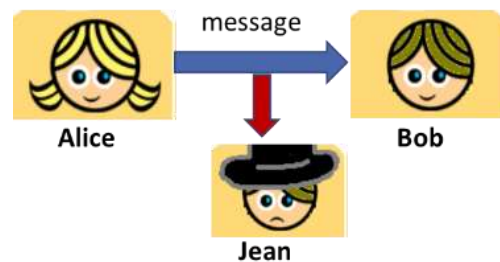
L'expéditeur (émetteur) et le destinataire (récepteur) sont deux entités importantes et reliées. Dans le cas normale :
Expéditeur(Alice) ⇒ message ⇒ destinataire(Bob)



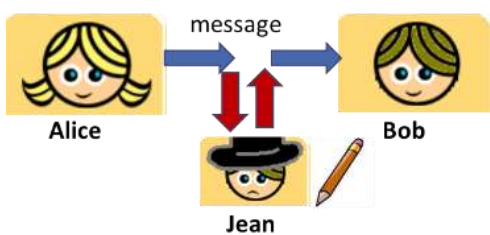
Un intermédiaire (intrus) peut agir sur un message de 4 manières :



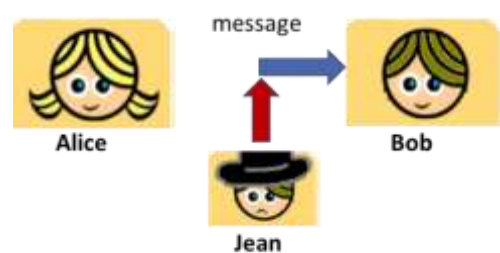
1. **intercepter + interrompre** : attaque sur la disponibilité : le message ne parvient pas à son destinataire



2. **intercepter + lire** : **attaque sur la confidentialité** : une information sensible parvient à une personne autre que son destinataire légitime.



3. **intercepter + modifier** : attaque sur l'intégrité



4. **intercepter + fabriquer** : attaque sur l'authenticité

Les menaces peuvent être classées en deux types :

- **Attaques passives** : Difficile à détecter car les données ne sont pas altérées :
 - L'opposant veut obtenir l'information transmise
 - Message courant (e-mail, téléphone)
 - Message encrypté (fréquence)
- ⇒ On peut juste le prévenir pas le détecter



- Attaques actives :
 - DoS (Denial of Service)
 - Impersonification : modification de l'identité de l'émetteur ou du récepteur
 - Altération des données (modification du contenu)
 - Destruction du message
 - Retardement de la transmission
 - ...

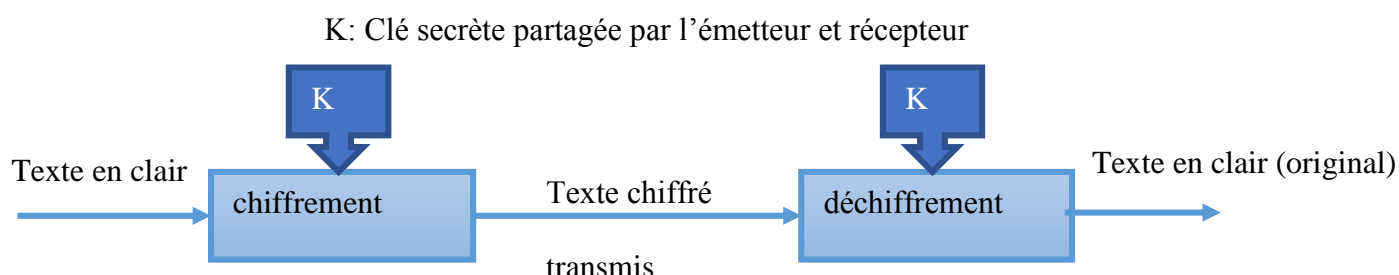
Chapitre 2 — Techniques cryptographiques classiques

1. Modèle de chiffrement conventionnel

Un schéma d'encrytion possède les cinq ingrédients suivants :

- Texte en clair (*Plaintext*)
- Algorithme d'encryption
- Clé secrète
- Texte chiffré (*Ciphertext*)
- Algorithme de décryption

La sécurité dépend de la sécurité de la clé et non pas de celle de l'algorithme, c.à.d. le secret concerne plutôt la clé et non pas l'algorithme.



- L'algorithme de chiffrement doit être suffisamment puissant pour s'assurer que le déchiffrement d'un texte encrypté doit être **impraticable**.
- La source produit du texte en clair $X = [X_1, X_2, \dots, X_M]$, de M lettres (blocs)
- Une clé $K = [K_1, K_2, \dots, K_J]$ est générée
- L'algorithme de chiffrement produira le texte chiffré $Y = [Y_1, Y_2, \dots, Y_N]$
- L'opération de chiffrement et celle de déchiffrement sont représentées par : $Y = E_K(X) \Leftrightarrow X = D_K(Y)$.

2. Techniques cryptographiques classiques

Les techniques cryptographiques classiques sont basées sur deux opérations : substitution et transposition

- **substitution** : consiste à remplacer des lettres par d'autres lettres
- **transposition** : consiste à arrangées les lettres suivant des ordres différents

les chiffrements peuvent être :

- **Monoalphabétique**: seule une substitution/ transposition est appliquée
- **Polyalphabétique**: plusieurs substitutions/ transpositions sont utilisées
- Combinaison des deux (*product cipher*)

2.1 Chiffrement monoalphabétique

Il s'agit de remplacer chaque caractère (lettre, nombre ou symbole) du texte en clair par un autre caractère.

Exemple : Texte en clair : **meet me after the toga party**

Texte chiffré : PHHW PH DIWHU WKH WRJD SDUWB

Dans ce cas-ci l'alphabet a été décalée de sorte que le Z est suivi par A (dans l'exemple le décalage est de **3 positions** à droite). Ce type de chiffrement est connu sous le nom de *chiffrement par décalage* ou "*Ceaser Cipher*"

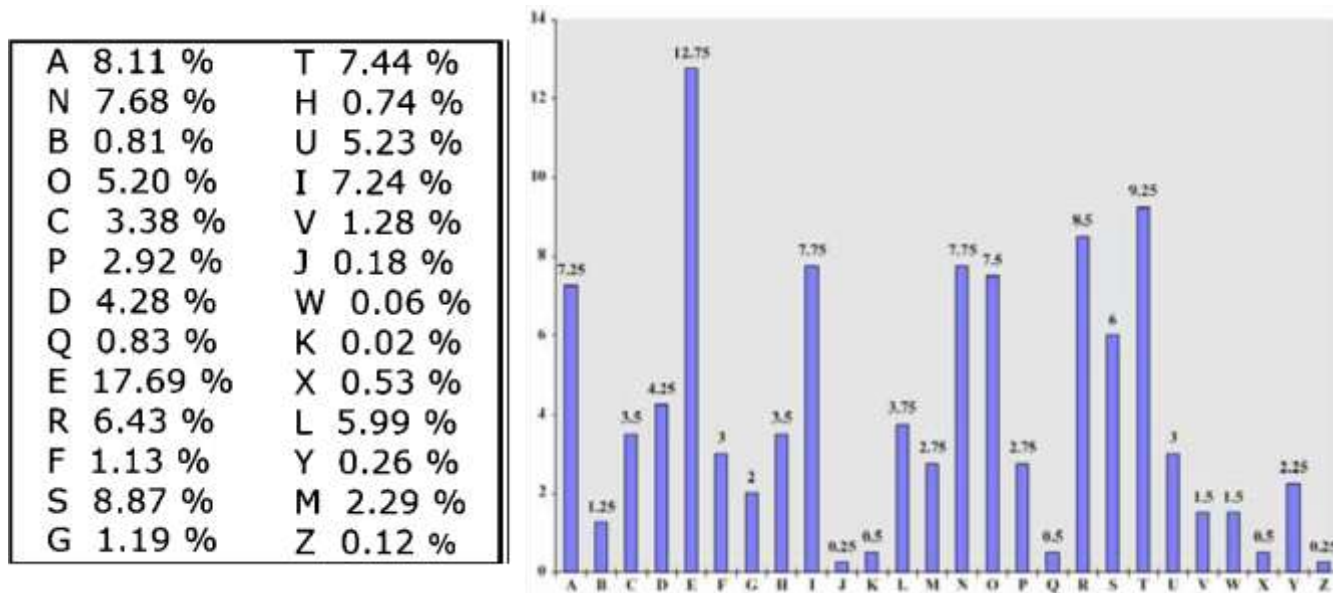
2.1.1 Substitution arbitraire

Consiste à remplacer des lettres par d'autres lettres.

- Alphabet en clair : a b c d e f g h i j k l m n o p q r s t u v x y z

Pour déchiffrer cet algorithme, 26! permutations sont possibles où 4×10^{26} clés possibles \Rightarrow attaque en force impossible (nécessite 6.4×10^6 années). Dons pour retrouver le texte clair, il faut envisager un autre type d'attaque, c'est l'attaque à l'aide de **l'analyse statistique**. (Fréquences des lettres ou des séquences de lettres)

Chaque langue possède une table de distribution de chaque lettre dans un texte en clair.



Distributions des lettres alphabétiques (françaises à gauche & anglaises à droite)

2.1.2 Chiffre de Playfair

Appelé aussi chiffre polygrammique, Il est Inventé par Sir **Charles Wheatstone** (1854) et a été popularisé par **Lyon Playfair**, il est utilisé pendant la 1^{ère} guerre mondiale. Le plus connu est le chiffrement multi-lettre où il traite les digrammes (1 unité = 2 caractères)

On dispose les 26 lettres de l'alphabet dans une matrice 5x5 tel que I et J = 1 lettre (occupent la même case) (c'est la version anglaise). Pour former les grilles de chiffrement, on utilise un **mot-clef secret** pour créer un alphabet désordonné avec lequel on remplissait la grille ligne par ligne.

■ Méthode de chiffrement

On chiffre le texte par groupes de deux lettres (bigrammes) en appliquant les règles suivantes :

- Remplir la matrice en commençant par la clé (MONARCHY).
- Si les deux lettres sont sur les coins d'un rectangle, alors les lettres chiffrées sont sur les deux autres coins.
- Si les deux lettres sont sur **la même ligne**, on prend les deux lettres qui les suivent immédiatement à **leur droite**. Exemple: CY \Leftrightarrow HB, PQ \Leftrightarrow QS.
- Si deux lettres sont sur **la même colonne**, on prend les deux lettres qui les suivent immédiatement **en dessous**. Exemple: ME \Leftrightarrow CL, KZ \Leftrightarrow TR.
- Si le **bigramme** est composé de deux fois la même lettre, on insère un nul (usuellement le X) entre les deux lettres pour éliminer ce doublon (Exp. balloon \Leftrightarrow ba lx lo on)

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/j	K
L	P	Q	S	T
U	V	W	X	Z

Pour déchiffrer, on applique les règles ci-dessus à l'envers.

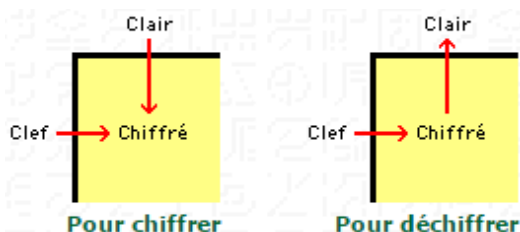
2.2 Chiffres à substitution polyalphabétique

Le chiffrement à substitution polyalphabétique consiste à utiliser de différents chiffres monalphabétiques au texte en clair. Il est composé d'un ensemble de règles de substitution monoalphabétiques et d'une clé. Il existe plusieurs chiffres : Chiffre de Bellaso, Chiffre de Porta, Chiffre de Beaufort, ... et le chiffre de Vigenère

2.2.1 Le chiffre de Vigenère

C'est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message.

Pour le chiffrement, La lettre de la clef est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut. La lettre chiffrée est à **l'intersection** de la ligne de



la lettre clef et de la colonne de la lettre claire. On repère la lettre de la clef dans la colonne la plus à gauche, on repère la colonne qui contient la lettre chiffrée dans cette ligne, la lettre déchiffrée est la 1^{ère} lettre de cette colonne.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières. Par exemple le E d'un texte clair peut être chiffré successivement (ITG...), ce qui rend inutilisable l'analyse des fréquences classique.

2.3 Chiffres à transposition

Un chiffre de transposition consiste à changer l'ordre des lettres, donc à construire des anagrammes. Cette méthode est connue depuis l'Antiquité, puisque les Spartes utilisaient déjà une scytale.



Un chiffre à transposition est un chiffre dans lequel les caractères du texte en clair **demeurent inchangés** mais dont les **positions respectives sont modifiées**. Du fait, une analyse statistique sur les chiffrements par transposition n'est pas utile, puisque seul l'ordre des symboles est différent ; les symboles restent les mêmes.

Pour chiffrer : on écrit le texte horizontalement sur une longueur fixe et on relève le texte chiffré verticalement. Une clé peut être ajoutée pour indiquer l'ordre des colonnes. **Pour déchiffrer** : Sur une feuille quadrillée, on utilise l'opération inverse.

2.3.1 Masque Jetable

Le système du masque jetable fut inventé en 1917 par Vernam et perfectionné par Mauborgne en 1918. C'est en fait un chiffre de Vigenère avec comme caractéristique que la clé de chiffrement a la même longueur que le message clair. Le masque jetable est le seul algorithme de cryptage connu comme étant indécryptable.

L'algorithme est simple : on ajoute le rang de la lettre à chiffrer au rang de la lettre correspondante du masque, le résultat mod 26 donne le rang de la lettre chiffrée. Le destinataire dispose d'un bloc identique et utilise le masque de la même manière pour déchiffrer chaque lettre du message chiffré. Le masque est utilisé une seule fois, pour un seul message.

Chapitre3 —Les attaques

1. Qu'est-ce que c'est ?

L'attaque (hacking) est un ensemble de techniques informatiques, visant à attaquer un réseau, un site, etc. Ces attaques sont diverses. On y retrouve :

- L'envoi de "bombes" logicielles.
- L'envoi et la recherche de chevaux de Troie.
- La recherche de trous de sécurité.
- Le détournement d'identité.
- La surcharge provoquée d'un système d'information (Flooding de Yahoo, eBay...).
- Changement des droits utilisateur d'un ordinateur.
- La provocation d'erreurs non gérées.

Les attaques peuvent être locales (sur le même ordinateur, voir sur le même réseau) ou distantes (sur internet, par télécommunication).

2. Le but du hacking

Les buts du hacking est divers. Selon les individus (les "hackers"), on y retrouve :

- Vérification de la sécurisation d'un système.
- Vol d'informations (fiches de paye...).
- Terrorisme.
- Espionnage "classique" ou industriel.
- Chantage.
- Manifestation politique
- Par simple "jeu", par défi.
- Pour apprendre.
- L'envoi de "bombes" logicielles.
- Etc.

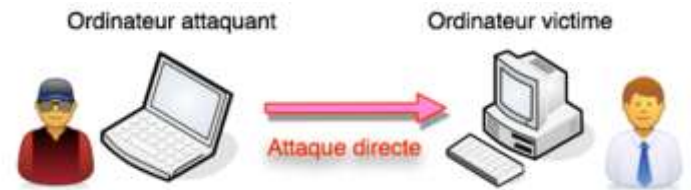
3. Les types d'attaques

Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes :

- Les attaques directes.
- Les attaques indirectes par rebond.
- Les attaques indirectes par réponses.

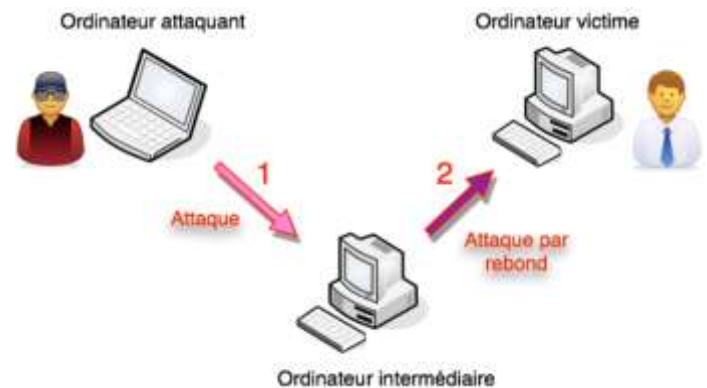
3.1 Les attaques directes

C'est la plus simple des attaques. La plupart des "script kiddies" utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime, ce qui permet souvent de remonter à l'origine de l'attaque en identifiant par la même occasion l'identité de l'attaquant.



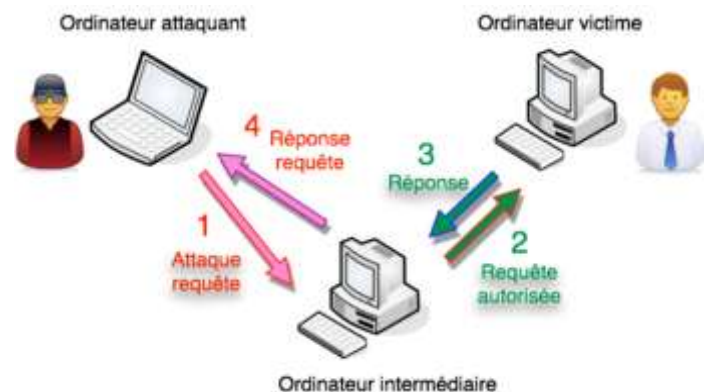
3.2 Les attaques indirectes par rebond

Cette attaque est la plus utilisée par les hackers. Le principe en lui-même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime d'où le terme de **rebond**. Le but du rebond est de masquer l'identité (@ IP) du hacker et éventuellement d'utiliser les ressources (CPU, bande passante...) de l'ordinateur intermédiaire car il est généralement plus puissant.



3.3 Les attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.



4. Exemples des Attaques

4.1 L'attaque Boink

L'attaque BOINK est un type d'attaque de Déni de Service (Denial of Service - DoS) utilisé sur les réseaux Internet contre les systèmes Win32. Elle consiste à envoyer des paquets UDP corrompus sur tous les ports ouverts. L'ordinateur victime ne gère pas ces paquets et provoque un plantage. Cette attaque cause le blocage système et le crash système. Pour s'en protéger, il faut mettre à jour l'OS et utiliser un firewall pour refuser les paquets UDP corrompus.

4.2 Le Mail Bombing

Le Mail Bombing consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires. L'objectif étant de saturer le serveur de mails, saturer la bande passante du serveur et des destinataires et rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.



Pour pouvoir effectuer le **mail bombing**, l'auteur de l'attaque doit se procurer un **logiciel** spécial permettant de la réaliser. Ce logiciel est fortement paramétrable, et offre différentes options : l'adresse d'émetteur du message, le sujet du message, le nombre de messages à envoyer, le serveur de mail à partir duquel les messages seront émis, le corps du message, l'adresse email de la victime... il peut

offrir la possibilité d'attacher une **pièce jointe** (ayant pour extension .com, .bat, .pif ou .exe) ce qui est une sérieuse menace, puisqu'elle permet à l'expéditeur d'insérer des virus et troyens dans les messages.

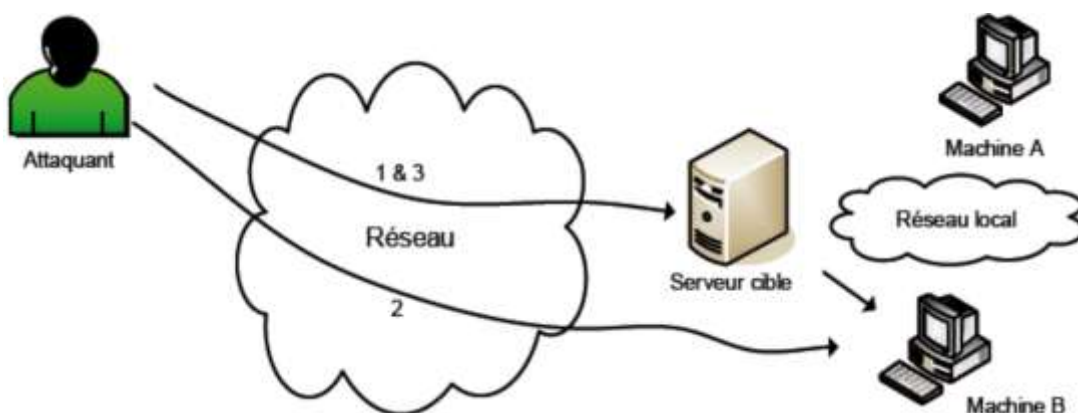
NB : Pour ne pas se retrouver contraint à changer votre adresse électronique, il faut impérativement éviter d'ouvrir une pièce jointe ayant pour extension l'une des extensions citées en dessus. On recommande également d'utiliser eremove pour éviter les mails bombers.

4.3 IP spoofing

L'**IP Spoofing** signifie **usurpation d'adresse IP**. Bien que cette attaque soit ancienne, certaines formes d'IP Spoofing sont encore d'actualité. Effectivement, cette attaque peut être utilisée de deux manières différentes :

- La première utilisation de l'IP Spoofing consiste à **falsifier la source d'une attaque**. Par exemple, lors d'une attaque de type déni de service, l'adresse IP source des paquets envoyés sera falsifiée pour éviter de localiser la provenance de l'attaque.
- L'autre utilisation de l'IP Spoofing va permettre de profiter d'une relation de **confiance entre deux machines** pour prendre la main sur l'une des deux. ➔ **on va s'intéresser ici à cette attaque.**

L'attaque IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible, ensuite il procède aux étapes illustrées dans la figure suivante pour mener à bien son attaque sur le serveur cible en utilisant l'adresse IP de la machine A.



1. **Trouver la machine de confiance** (son @ IP) qu'accepte le service du serveur cible.
2. **Mettre hors service cette machine de confiance** (avec un SYN Flooding par exemple) pour éviter qu'elle ne réponde aux paquets éventuellement envoyés par le serveur cible.
3. Le pirate falsifie son adresse IP en la remplaçant par celle de la machine invalidée et envoie une demande de connexion au serveur cible.
4. **Le serveur envoie une trame SYN|ACK** à la machine qu'il pense être l'émettrice. Celle-ci ne pouvant répondre, le pirate acquitte cette connexion par une trame ACK, avec le numéro de séquence prévu. **Il établit de la sorte en toute impunité la connexion avec le serveur cible.**

NB : Cette attaque est assez difficile à effectuer, car elle se réalise en aveugle, le pirate ne recevant pas les données transmises par le serveur. Il doit donc maîtriser parfaitement les protocoles pour savoir ce qu'attend le serveur à tout moment.

4.4 DNS spoofing

L'objectif de cette attaque est de rediriger, à leur insu, des Internautes vers des sites pirates. Pour la mener à bien, le pirate utilise des faiblesses du protocole DNS et/ou de son implémentation au travers des serveurs de nom de domaine. Le but du pirate est de faire correspondre l'adresse IP d'une machine qu'il contrôle à un nom réel et valide d'une machine publique. Il existe deux principales attaques de type DNS Spoofing ; DNS ID Spoofing et DNS Cache Poisoning.

4.4.1 Description de l'attaque DNS ID Spoofing

Si une machine A veut communiquer avec une machine B, la machine A a obligatoirement besoin de l'adresse IP de la machine B. si A n'a pas l'adresse ip de B, elle va utiliser le protocole DNS pour l'obtenir. Pour ceci, la machine A envoie une requête DNS (nom-site, num_id) au serveur DNS, déclaré au niveau de A, demandant la résolution du nom de B en son adresse IP. Ainsi, le serveur DNS enverra la réponse à cette requête avec le même numéro d'identification.

L'attaque consiste à récupérer ce numéro d'identification pour pouvoir envoyer une réponse falsifiée avant le serveur DNS. Ainsi, la machine A utilisera, sans le savoir, l'adresse IP du pirate et non celle de la machine B initialement destinataire.



4.4.2 DNS Cache Poisoning

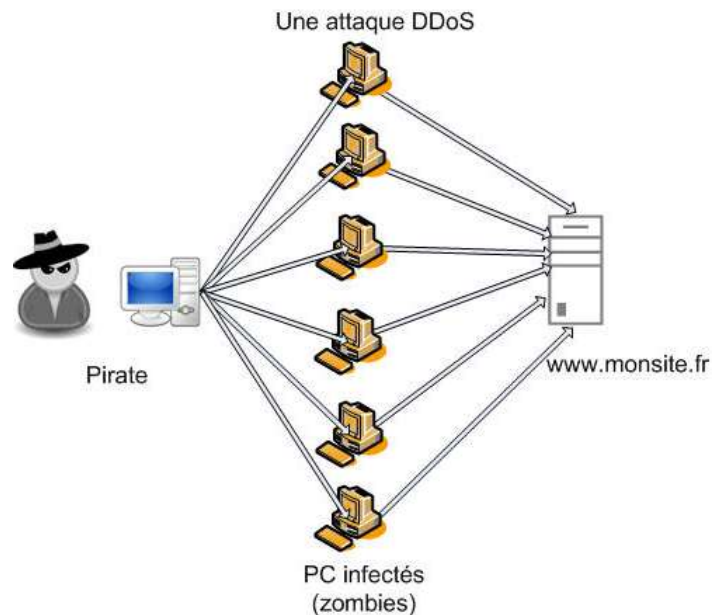
Les serveurs DNS possèdent un cache permettant de garder pendant un certain temps la correspondance entre un (nom de machine, son @ IP). Un serveur DNS n'a les correspondances que pour les machines du domaine sur lequel il a autorité. Pour les autres machines, il contacte le serveur DNS ayant autorité sur le domaine auquel appartiennent ces machines. Ces réponses, pour éviter de sans cesse les redemander aux différents serveurs DNS, seront gardées dans ce cache.

Le DNS Cache Poisoning consiste à corrompre ce cache avec de fausses informations. Pour cela le pirate doit avoir sous son contrôle un nom de domaine (par exemple fourbe.com) et le serveur DNS ayant autorité sur celui-ci ns.fourbe.com. Le pirate envoie une requête vers le serveur DNS cible demandant la résolution du nom d'une machine du domaine fourbe.com (ex.: www.fourbe.com). Le serveur DNS cible relaie cette requête à ns.fourbe.com (puisque c'est lui qui a autorité sur le domaine fourbe.com), le serveur DNS du pirate enverra alors, en plus de la réponse, des enregistrements additionnels (dans lesquels se trouvent les informations falsifiées ex. machine publique associé à une adresse IP du pirate), Les enregistrements additionnels sont alors mis dans le cache du serveur DNS cible. Et comme résultat, une machine faisant une requête sur le serveur DNS cible demandant la résolution d'un des noms corrompus aura pour réponse une adresse IP autre que l'adresse IP réelle associée à cette machine.

4.5 Dénî de service

Le déni de service, ou DoS (Denial of Service), est une attaque qui vise à rendre indisponible un service, un système ou un réseau. Ces attaques s'appuient généralement sur une faiblesse d'implémentation, ou bogue, ou sur une faiblesse d'un protocole. Il peut s'agir de :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier ;
- également le fait d'envoyer des milliards d'octets à un box internet.



Les attaques par déni de service non distribuées peuvent être contrées en identifiant l'adresse IP de la machine émettant les attaques et en la bannissant au niveau du pare-feu ou du serveur. Les paquets IP provenant de la machine hostile sont dès lors rejetés sans être traités empêchant que le service du serveur ne soit saturé et ne se retrouve donc hors-ligne. Par contre les attaques par DDoS sont plus difficiles à contrer (ce type est utilisé pour diminuer les possibilités de stopper l'attaque). Celle-ci émanant de nombreuses machines hostiles aux adresses différentes, bloquer les adresses IP limite l'attaque mais ne l'arrête pas.

NB : En réalité, la prévention doit plus porter sur le renforcement du niveau de sécurité des machines connectées au réseau pour éviter qu'une machine puisse être compromise que sur la protection des machines cibles (les serveurs Web).

4.6 Web bug

Web bug connu aussi sous nom de Pixel invisible ou pixel espion est une image GIF invisible de la taille d'un pixel insérée dans une page Web ou un courrier électronique en HTML, qui s'active lors du téléchargement de la page et lance une requête au serveur pour collecter des informations sur l'internaute (l'adresse IP, l'email, le nom de l'ordinateur hôte, ainsi que le nom et la version du système d'exploitation et du navigateur utilisés) à son insu. Ces informations seront transmises à un serveur distant pour exploitation ultérieure, notamment par des agences de marketing

Exp d'email: `` : la requête de téléchargement de l'image vient confirmer la lecture du message et la **validité** de votre adresse.

4.7 Les Virus

Un virus est un logiciel capable de s'installer sur un ordinateur à l'insu de son utilisateur légitime. Le terme virus est réservé aux logiciels qui se comportent ainsi avec un but malveillant, parce qu'il existe des usages légitimes de cette technique dite de code mobile ; les appliquelettes Java et les procédures JavaScript sont des programmes qui viennent s'exécuter sur votre ordinateur en se

chargeant à distance depuis un serveur Web que vous visitez, sans que toujours vous en ayez conscience, et en principe avec un motif légitime.

Pour infecter un système, un virus agit de la façon suivante : il se présente sous la forme de quelques lignes de code en langage machine binaire qui se greffent sur un programme utilisé sur le système cible, afin d'en modifier le comportement. Le virus peut être tout entier contenu dans ce greffon, ou il peut s'agir d'une simple amorce, dont le rôle va être de télécharger un programme plus important qui sera le vrai virus.

Une fois implanté sur son programme-hôte, le greffon possède aussi en général la capacité de se recopier sur d'autres programmes, ce qui accroît la virulence de l'infection et peut contaminer tout le système ; la désinfection n'en sera que plus laborieuse.

4.7.1 Virus réticulaire (botnet)

La cible d'un virus informatique peut être indirecte : il y a des exemples de virus qui se propagent silencieusement sur des millions d'ordinateurs connectés à l'Internet, sans y commettre le moindre dégât. Puis, à un signal donné, ou à une heure fixée, ces millions de programmes vont se connecter à un même serveur Web, ce qui provoquera son effondrement. C'est ce qu'on appelle un déni de service distribué (*Distributed Denial of Service, DDoS*). Un tel virus s'appelle en argot SSI un bot, et l'ensemble de ces virus déployés un botnet. Les ordinateurs infectés par des bots sont nommés zombis.

4.7.2 Les Vers

Un ver (*worm*) est une variété de virus qui se propage par le réseau. Son but est de grignoter des ressources système (CPU, mémoire, espace disque, bande passante...). En fait, alors qu'il y a quelques années les virus n'étaient pas des vers (ils ne se propageaient pas par le réseau) et les vers n'étaient pas des virus (ils ne se reproduisaient pas), aujourd'hui la confusion entre les deux catégories est presque totale. Une machine infectée par des vers: Ralentissement système, Blocage système, Crash système, Pertes de données ...

4.7.3 Cheval de Troie

Un cheval de Troie (*Trojan horse*) est un logiciel qui se présente sous un jour honnête, utile ou agréable, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses. Une machine infectée par des chevaux de Troie a comme Symptômes : Activité anormale de la carte réseau ou du disque dur (des données sont chargées en l'absence d'activité de la part de l'utilisateur) ou du modem, Réactions curieuses de la souris, Ouvertures impromptues de programmes, Plantages répétés, Redémarrage répété du système, Écran ou fenêtres avec des messages inhabituels ...

4.7.4 Porte dérobée

Une porte dérobée (*backdoor*) est un logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie, qui donne à un agresseur extérieur accès à l'ordinateur victime, par le réseau.

4.7.5 Bombe logique

Une bombe logique est une fonction, cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou lorsque surviendra un certain événement. Cette fonction produira alors des actions indésirées, voire nuisibles.

4.7.6 Logiciel espion

Un logiciel espion ou espioiciel (Spywares), comme son nom l'indique, collecte à l'insu de l'utilisateur légitime des informations au sein du système où il est installé, et les communique à un agent extérieur, par exemple au moyen d'une porte dérobée. Ils se trouvent généralement dans le code d'un programme que l'utilisateur téléchargera innocemment sur internet. Dans un même programme, il peut y avoir plusieurs routines parasites différentes, ayant chacune une fonction déterminée exp: prog de messagerie contient une routine envoie une copie de chaque msg à une adresse sans laisser de trace dans la boîte éléments envoyés de l'email dupliqué.

NB : Sans vouloir sembler paranoïaque, il est donc important de garder en mémoire que tout exécutable est potentiellement infecté d'un espioiciel.

4.7.6.1 keylogger

Une variété particulièrement toxique de logiciel espion est le *keylogger* (espion dactylographique ou encore enregistreurs **de frappe**), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet au pirate ; il capte ainsi notamment identifiants, mots de passe et codes secrets (un fichier log généralement crypté, contenant tous les renseignements collectés)

NB: il est impossible à l'heure actuelle de surfer en étant certain que nos informations ne sont pas transmises. Il n'existe aucun moyen de s'assurer qu'un ordinateur connecté à internet ne soit pas à même d'envoyer à notre insu des éléments non désirés.

4.8 Logiciel de sécurité non autorisé

Un logiciel de sécurité non autorisé tente de vous faire croire que votre ordinateur est infecté par un virus et vous invite en général à télécharger ou à acheter un produit qui élimine les virus. Les noms de ces produits contiennent souvent des mots tels que antivirus, bouclier, sécurité, protection ou vérificateur, ce qui les fait paraître légitimes. Ils s'exécutent souvent immédiatement après leur téléchargement ou lors du prochain démarrage de votre ordinateur.

Les logiciels de sécurité non autorisés peuvent empêcher l'ouverture d'applications, telles qu'Internet Explorer. Ils peuvent également afficher des fichiers Windows légitimes et importants comme étant infectés. Des messages contextuels ou des messages d'erreur classiques peuvent contenir les mentions suivantes :

Avertissement !
Votre ordinateur est infecté !
Cet ordinateur est infecté par des logiciels espions et de publicité.



4.9 Courrier électronique non sollicité (spam)

Les messages électroniques non sollicités contiennent généralement de la publicité, le plus souvent pour des produits pharmaceutiques destinés à améliorer les dimensions et les performances de certaines parties du corps humain, des produits financiers ou des procédés d'enrichissement rapide. Parfois il s'agit d'escroqueries pures et simples, qui invitent le lecteur à accéder à un site qui va lui extorquer son numéro de carte bancaire sous un prétexte plus ou moins vraisemblable, cela s'appelle le phishing.

4.10 Social engineering

L'**ingénierie sociale** (*social engineering*) est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs.

En utilisant les moyens usuels (téléphone, email...) et en usurpant une identité, un pirate cherche à obtenir des renseignements confidentiels auprès du personnel de l'entreprise en vue d'une intrusion future. Seule une formation du personnel permet de se protéger de cette attaque. Il est important, de la part d'une entreprise, de **former le personnel** à ce problème. Un bon hacker s'attaquera à la personne la plus faible de l'entreprise, à savoir le personnel non technique (secrétaires, comptables...) et les personnes récemment recrutées.

5. Protections

5.1 FORMATION DES UTILISATEURS

L'être humain est le maillon de la sécurité le plus faible dans un système de sécurité et on considère généralement que la majorité des problèmes de sécurité sont situés entre la chaise et le clavier !

Discrétion : la sensibilisation des utilisateurs à la faible sécurité des outils de communication et à l'importance de la non divulgation d'informations par ces moyens est indispensable. En effet il est souvent trop facile d'obtenir des mots de passe par téléphone ou par e-mail en se faisant passer pour un membre important de la société.

Virus : plusieurs études récentes montrent que 1/3 des utilisateurs ouvriraient encore une pièce jointe d'un courrier nommée « i love you » et que la moitié ouvriraient une pièce nommée « ouvrez-ça » ou similaire... ! L'information régulière du personnel est nécessaire, attention toutefois aux rumeurs (hoax).

Charte : l'intérêt principal d'une charte d'entreprise est d'obliger les employés à lire et signer un document précisant leurs droits et devoirs et par la même de leur faire prendre conscience de leur responsabilité individuelle

5.2 POSTE DE TRAVAIL

Le poste de travail reste un maillon faible de la sécurité. Le projet TCG (Trusted Computing Group) visant à sécuriser les équipements et communications informatiques en assignant une signature à chaque objet informatique (logiciel, document, ...), et à déléguer à un *tiers de confiance* la tâche de vérifier si l'objet manipulé est autorisé à être utilisé sur le système informatique local ou non ;

5.2.1 LES ANTIVIRUS

Un ANTIVIRUS est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier. (S'il s'avère que c'est bien un programme nuisible, il doit décider quelle est la meilleure action à envisager en fonction des dégâts causés) qui peut être :

- Tenter de réparer le fichier endommagé en éliminant le virus.
- Effectuer la suppression du fichier contaminé.
- Déplacer le fichier dans une zone de quarantaine afin qu'il ne puisse être accessible aux autres utilisateurs et logiciels. Ceci permet d'éviter que le virus se répande (par autoréplication), et permet éventuellement de réparer le fichier ultérieurement ;

L'antivirus surveille en permanence, en tâche de fond, toutes les activités de l'ordinateur, en essayant de minimiser l'impact de cette surveillance sur les performances du système. Le but étant de limiter la gêne occasionnée pour l'utilisateur tout en gardant la possibilité de prendre des décisions importantes voire vitales en cas de besoin. Pour détecter un virus, il se sert de plusieurs techniques :

- Détection de la signature
- La détection par le comportement
- Le contrôle d'intégrité
- L'analyse heuristique

5.2.1.1 La détection par la signature

On l'appelle aussi **scan** ou **scanning**. C'est la méthode la plus ancienne et la plus utilisée. Cette méthode consiste à analyser le disque dur à la recherche de la **signature (morceau de code ou une chaîne de caractères du virus qui permet de l'identifier)** du virus, qui est présent dans la base de données du logiciel, si celui-ci est à jour et s'il connaît ce virus.

Votre logiciel de protection doit donc être mis à jour régulièrement pour être informé des nouvelles menaces qui apparaissent chaque jour sur l'Internet et ainsi maintenir son efficacité. L'avantage de la technique du scan est qu'elle permet de détecter les virus avant leur exécution en mémoire, dès qu'ils sont stockés sur le disque et qu'une analyse est exécutée. Cependant cette méthode n'est pas efficace contre les nouveaux virus ou les virus dits **polymorphes**, dont la signature change à chaque répllication.

5.2.1.2 La détection par le comportement

Une autre approche pour localiser les virus consiste à détecter les comportements suspects des programmes. Par exemple, si un programme tente d'écrire des données sur un programme exécuté, modifier/supprimer des fichiers système l'antivirus détectera ce comportement suspect et en avisera l'utilisateur qui choisira les mesures à suivre. Contrairement à l'approche précédente, la méthode du comportement suspect permet d'identifier des virus très récents qui ne seraient pas encore connus dans le dictionnaire de l'antivirus. Toutefois, le fait que les utilisateurs soient constamment avertis de fausses alertes peuvent les rendre insensibles aux véritables menaces.

5.2.1.3 La détection par le contrôle de l'intégrité

Vérifier l'intégrité d'un fichier consiste à contrôler qu'il n'a pas été modifié ou altéré au cours du temps. L'antivirus, pour contrôler l'intégrité des fichiers, va stocker un fichier central recensant l'ensemble des fichiers présents sur le disque auxquels il aura associé des informations (La taille, La date et heure de dernière modification, La somme de contrôle (CRC : code de redondance cyclique)) éventuelle qui peuvent changer lorsque le fichier est modifié.

Lorsqu'une analyse est effectuée (ou à l'ouverture du fichier si l'antivirus réside en mémoire), l'antivirus recalcule la somme de contrôle et vérifie que les autres paramètres n'ont pas été modifiés. Si une anomalie se présente, l'utilisateur est informé. Le point faible de cette technique est que les virus les plus récents ne modifient pas les dates d'accès des fichiers, ou les rétablissent après avoir les avoir infecté

5.2.1.4 L'analyse heuristique

C'est la méthode la plus puissante et la plus récente qui est mise en avant par les meilleurs antivirus car elle permet de détecter d'éventuels virus inconnus. Elle cherche à détecter la présence d'un virus

en analysant le code d'un programme inconnu (en simulant son fonctionnement). Elle provoque parfois de fausses alertes. L'Antivirus simule l'exécution d'un programme inconnu dans une zone sûre de disque dur pour voir ce qu'il pourrait se passer, ces vérifications provoquent parfois de fausses alertes, on appelle cela des faux positifs

5.2.2 Méthodes d'éradication du Virus

- Réparer le fichier : L'antivirus doit être capable de réparer un fichier infecté. Mais ce n'est pas toujours possible.
- Supprimer le fichier : Si l'antivirus n'est pas capable de réparer le fichier, vous pouvez le supprimer. On conseille cette option si le fichier n'est pas important, sinon, mettez-le en quarantaine.
- Mise en quarantaine du fichier infecté : C'est une solution d'attente. les fichiers sont placés dans un dossier isolé et sûr sur le disque afin que le programme malveillant ne puisse agir. Au fur et à mesure des mises à jour de sa base virale, il pourra éventuellement le réparer / supprimer et même parfois décider que le fichier incriminé n'est pas dangereux et le faire sortir de cette quarantaine.

6. Conclusion

On va conclure par une évidence : on ne le répétera jamais assez, le maillon faible de votre protection c'est...Vous !