SÉCURITÉ INFORMATIQUE

3ème Année Informatique

Chapitre 1 :

Introduction à la sécurité

Introduction

• Un système d'information est une organisation d'activités consistant à acquérir, stocker, traiter, et diffuser les informations. Un des moyens techniques pour faire fonctionner un système d'information est d'utiliser des systèmes informatiques.

• Assurer la sécurité de l'information implique ainsi d'assurer la sécurité des systèmes informatiques.

• Le problème de la protection des informations sur les ordinateurs est devenu encore plus critique et difficile depuis l'adoption de l'Internet. L'Internet est devenu la route principale à la pénétration aux systèmes par des utilisateurs non autorisés qui peuvent effectuer des actions malveillantes.

• Il est donc essentiel de connaître les ressources du système à protéger et mettre en œuvre des mécanismes de protection.

1. Définitions

1. Sécurité informatique

C'est l'ensemble des moyens techniques, organisationnels, juridiques et humains mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

2. Sécurité et sûreté

La sécurité informatique concerne deux domaines :

• **« Sûreté = Safety (en anglais) » :** protection de systèmes informatiques contre les accidents dus à l'environnement et les défauts du système.

• **« Sécurité = Security (en anglais) »** : protection des systèmes informatiques contre des actions malveillantes intentionnelles.

2. Principaux concepts de sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini. Afin de bien comprendre ces malveillances informatiques, il est nécessaire de définir certains termes :

• **Vulnérabilité :** une vulnérabilité (en anglais « vulnerability », appelée parfois faille ou brèche) est un point où un système est sensible à une attaque malveillante. Il s'agit d'une faiblesse de sécurité de nature logique ou physique pouvant être exploitée pour causer des pertes ou des dommages.

• **Menace :** une menace (en anglais « threat ») représente le type d'action malveillante susceptible de nuire à un système informatique en exploitant ses vulnérabilités (ses faiblesses) de sécurité. Une menace est un danger possible pour le système.

•**Attaques :** Une attaque est une tentative volontaire de violer une ou plusieurs propriétés de sécurité.

• **Contre-mesure :** c'est l'ensemble des actions mises en œuvre en prévention de la menace.

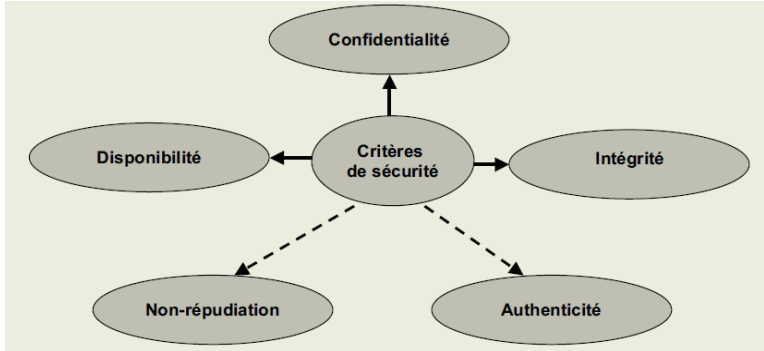
• **Risque :** Il signifie la probabilité qu'une menace exploitera une vulnérabilité du système. La définition du risque dépend de la notion de menace associée ou non à des vulnérabilités. On peut formaliser le risque comme suit:

$$Risque = \frac{Menace \times Vulnérabilité}{Contre\ mesure}$$

3. Objectifs de la sécurité informatique

Les objectifs (propriétés, exigences, services,, …) de la sécurité informatique caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité.

Cinq principaux objectifs à garantir :



1. Confidentialité

C'est la propriété qui assure que seuls les utilisateurs autorisés, dans des conditions prédéfinies, ont accès aux informations. C'est-à-dire garder les informations secrètes sauf pour les personnes auxquels elles sont destinées. L'un des moyens pour garantir la confidentialité des données est le chiffrement des données et la cryptographie.

2. Authentification

C'est la propriété qui assure la vérification et la confirmation de l'identité des entités qui s'échangent des informations, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Parmi les moyens utilisés pour garantir l'authentification sont les login/mot de passe, certificats numériques, etc.

3. Intégrité

C'est la propriété qui assure que les données ne sont pas corrompues ni modifiées de façon non autorisée. L'un des moyen pour assurer l'intégrité est l'utilisation des empreintes digitales.

4. Disponibilité

C'est la propriété qui assure que les données ou les services d'un système sont accessibles au moment voulu par les utilisateurs autorisés.

5. Non répudiation

C'est la propriété qui assure que l'auteur d'un acte ne peut ensuite nier l'avoir fait, il en assume la responsabilité. Par exemple empêcher l'émetteur ou le récepteur de nier la transmission ou la réception d'un message.

4. Classification des menaces

Avant de pouvoir mettre en œuvre une solution de sécurité, il faut d'abord commencer par connaître les différents dangers et leurs motivations afin de prévoir la façon de les protéger et limiter les risques.

Les différentes menaces qui existent peuvent être classifiées selon plusieurs classes :

- **selon la technologie,**
- **selon l'intention,**
- **selon le comportement,**
- **selon l'action.**

4.1. La classification selon la technologie

1. Menace non Informatique

• Risques matériels accidentels :

Incendie, explosion, inondation, tempête, foudre.

• Vol et sabotage de matériels :

Vol d'équipements matériels, destruction d'équipements, destruction de supports de sauvegarde.

• Autres risques :

Tout ce qui peut entrainer des pertes financières dans une société. Pertes plutôt associées à l'organisation, à la gestion des personnels (départ de personnels stratégiques, grèves, etc.).

4.1. La classification selon la technologie

2. Menace Informatique

Une menace informatique représente un danger lié aux ressources techniques. Ces types de menaces sont les plus courantes et représentent parfois les plus grands dangers pour la réalisation d'une attaque.

Exemples : virus, panne de serveurs, …

4.2. Classification selon l'intention

1. Menaces non intentionnelles

Les menaces non intentionnelles sont les menaces qui sont réalisées de façon accidentelle sans préméditation ou l'intention de nuire. Elles peuvent être :

- Des pannes ou dysfonctionnements matériels.
- Des pannes ou dysfonctionnements logiciels.
- Des erreurs : ces erreurs regroupent :
  - ✓Les erreurs d'exploitation : comme les oublis de sauvegarde.
  - ✓Les écrasements de fichiers.
  - ✓Les erreurs de manipulation des informations.
  - ✓Les erreurs de saisie.
  - ✓Les erreurs de transmission.
  - ✓Les erreurs de conception des applications.

4.2. Classification selon l'intention

2. Menaces Intentionnelles

Les menaces intentionnelles sont réalisées dans l'intention de nuire. Elle regroupe l'ensemble des actions malveillantes faites de façon délibérée (Malveillance Informatique).

Exemple :

Virus, Vers, Cheval de Troie, logiciel espion, spam, ...

4.3. Classification selon le comportement

1. Menaces Actives

Ce type de menaces implique la modification ou création des données ou des messages, afin d'introduire de fausses informations ou perturber le bon fonctionnement d'un système. Une menace active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ce type de menaces, bien qu'elles soient détectables (permettant ainsi une réponse adéquate).

Exemples :

• Virus qui détruit des données,

• Modification d'un e-mail par une tierce personne, . . .

4.3. Classification selon le comportement

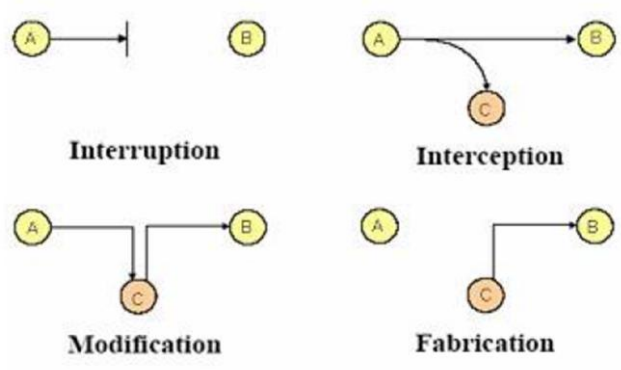
2. Menaces Passives

Une menace passive est une attaque qui ne modifie pas l'état des données ou du système. Elle consiste à écouter sans modifier les données ou le fonctionnement du système. Elles sont généralement indétectables mais une prévention est possible.

Une menace passive est souvent réalisée afin d'obtenir des données par écoute indiscrètes ou surveillance des transmissions.

4.3. Classification selon l'action

Cette classe de menaces regroupe les types répertoriés selon l'action effectuée lors de la réalisation de la menace. Il affecte le processus de communication et regroupe les menaces suivantes :



4.3. Classification selon l'action

1. Menace d'interruption

Dans ce type de menace un composant du système est détruit ou devient indisponible ou inutilisable. Ainsi, cette menace provoque une obstruction quelconque lors du processus de communication entre un ou plusieurs systèmes et ces systèmes deviennent inutilisables, ce qui entraîne un gaspillage des ressources du système.

2. Menace d'interception

Pour ce type, une tierce partie non autorisée obtient un accès à une ressource. Cette partie tierce peut être une personne, un programme ou un système informatique. Bien qu'une perte puisse être découverte assez rapidement.

4.3. Classification selon l'action

3. Menace de modification

Une tierce partie non autorisée obtient accès à une ressource et la modifie de façon presque indétectable. L'intégrité du message est perdue par ce type de menace puisque le destinataire ne peut pas recevoir le message exact envoyé par la source.

4. Menace de fabrication

Pour ce type, une tierce partie non autorisée obtient un accès à une ressource. Cette partie tierce peut être une personne, un programme ou un système informatique. Bien qu'une perte puisse être découverte assez rapidement.

4.3. Classification selon l'action

3. Menace de modification

Une tierce partie non autorisée obtient accès à une ressource et la modifie de façon presque indétectable. L'intégrité du message est perdue par ce type de menace puisque le destinataire ne peut pas recevoir le message exact envoyé par la source.

4. Menace de fabrication

Pour ce type, une tierce partie non autorisée obtient un accès à une ressource. Cette partie tierce peut être une personne, un programme ou un système informatique. Bien qu'une perte puisse être découverte assez rapidement.

5.Les différents types d'attaques

Les attaques informatique représente les différentes menaces informatiques intentionnelles. On peut regrouper ces attaques en quatre catégories : logiciels malveillants, attaques par messagerie, exploit et intrusion et attaques Web.

5.1. Logiciels malveillants

Un logiciel malveillance (malware en anglais) est aussi dénommé logiciel nuisible ou programme malveillant. C'est une application développée dans le but de nuire à un système informatique, sans le consentement de l'utilisateur. Il existe une multitude de logiciels malveillants parmi lesquels on retrouve les virus, ver, trojan, rootkit, Bombes logiques, spyware, …

5.Les différents types d'attaques

5.1.1. Virus

Un virus est un programme illicite qui s'insère dans des programmes ou fichiers légitimes appelés hôtes. Il est capable de se dupliquer automatiquement sur d'autres ordinateurs (disquette, CD, Flash disque, web, ...) et peut avoir comme effet plus ou moins grave de perturber le fonctionnement de l'ordinateur infecté.

5.1.2. Ver Informatique (Worm)

Un ver informatique est un virus réseau. C'est un programme malveillant qui peut se reproduire et se déplacer à travers un réseau sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc…). Il exploite les ressources système de l'ordinateur infecté afin d'espionner, installer une porte dérobée, détruire des données, envoyer de multiples requêtes, …

Les vers actuels se propagent principalement grâce à la messagerie.

5.Les différents types d'attaques

5.1.3. Cheval de Troie (trojan)

Un trojan est un programme malveillant placé dans un programme sain. Il est programmé pour être installé de manière invisible par des utilisateurs naïfs, ou des programmes illicites afin d'avoir un contrôle sur l'ordinateur de la victime.

Il peut servir à voler des mots de passe, copier des données sensibles, créer une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur (ouvrir un port).

5.1.4. Bombes logiques

C'est un programme malveillant ne pouvant se reproduire, souvent associé avec un cheval de Troie. Il est le plus souvent destructeur. Une bombe logique contient une partie de code conditionnelle qui explosera une fois la condition réalisée (temps, date, action, signal, …) et non lors de l'installation de la bombe logique. Par exemple : un cheval de Troie associé à un écran de veille, la bombe logique explosera après quelques heures de veille.

5.Les différents types d'attaques

5.1.5. Espiongiciel (spyware)

Un espiongiciel (en anglais spyware) est un programme espion chargé de recueillir des informations sur l'utilisateur de l'ordinateur dans lequel il est installé. Il s'installe généralement en même temps que d'autres logiciels (la plupart du temps des freewares ou sharewares, souvent légaux cités dans la licence).

Un spyware enregistre toute l'activité de l'ordinateur infecté et la retransmet à quelqu'un d'autre. Il permet de tracer des URL des sites visités, traquer des mots-clés saisis dans les moteurs de recherche, analyser des achats réalisés via internet, voire les informations de paiement bancaire, . . .

5.1.6. Sniffer

Un sniffer est un type particulier d'espiogiciel qui permet d'écouter et de récupérer les données circulant sur le réseau (mots de passe, carte bancaires, …).

5.Les différents types d'attaques

5.1.7. Keylogger

Un keylogger (enregistreur de touches) est un programme espion chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur.

4.1.8. Rançongiciel (Ransomware)

C'est un logiciel malveillant (virus, ver ou cheval de Troie) qui prend en otage des données personnelles. Pour cela, il chiffre des données personnelles puis demande à la victime d'envoyer de l'argent en échange de la clé de déchiffrement. Il peut aussi bloquer l'accès à la machine jusqu'à ce que l'utilisateur paie une somme d'argent.

4.1.9. Logiciel publicitaire (Adware)

C'est un programme gratuit financé par des publicités qui s'affichent dans des fenêtres indépendantes ou dans une barre d'outils sur l'ordinateur ou dans le navigateur.

La plupart des adwares sont désagréables, mais sûrs. Cependant, certains sont utilisés pour recueillir des informations personnelles, les sites web visités. . .

5.Les différents types d'attaques

5.2. Malveillance par Messagerie

Les malveillances par messagerie regroupent toutes les menaces informatiques intentionnelles ciblant les comptes de messageries, les e-mails ou les échanges de courriers électroniques. On y distingue principalement trois types : les spams, les courriels hameçonnage et les canulars.

5.2.1. Pourriel (spam)

Un spam (pourriel, junk mail, courrier indésirable) est l'envoi massif de courrier électronique à des destinataires ne l'ayant pas sollicité.

Les spammeurs collectent généralement les adresses électroniques sur internet (dans les forums, sur les sites internet, dans les groupes de discussion, …).

5.Les différents types d'attaques

5.2.2. Hameçonnage (phishing)

L'hameçonnage est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès des utilisateurs.

Les utilisateurs reçoivent un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce (copie conforme du site original).

5.2.3. Canular (Hoax)

Un canular est un courriel électronique propageant de fausses informations et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues. En apparence les canulars ne sont nocifs mais ils peuvent avoir d'autres conséquences telles que la congestion des réseaux, la diffusion de fausses rumeurs et l'encombrement des boites aux lettres électroniques avec la diffusion massive de courriels.

5.Les différents types d'attaques

5.3. Exploit et intrusion

Ce type de malveillance informatique regroupe les techniques et logiciels visant à s'introduire dans un système et l'exploiter à des fins personnelles ou mal intentionnés.

5.3.1. Porte dérobée (backdoor)

Une porte dérobée (backdoor en anglais) représente une fonctionnalité secrète d'un logiciel permettant de surveiller ou de prendre le contrôle d'un ordinateur. Elle est due à une faute de conception accidentelle ou intentionnelle (cheval de Troie généralement). Par exemple une porte dérobée pourrait être une faille dans le SGBD MySQL qui permet de se connecter en tant qu'administrateur.

5.3.2. Intrusion

Une intrusion représente une technique qui permet d'infiltrer un système informatique ou un réseau afin de réaliser une attaque. Elle peut être réalisée en utilisant les outils de malveillance logiciels ou de messagerie.

5.Les différents types d'attaques

5.3.3. Exploit

Un exploit est un programme permettant à un attaquant d'exploiter une faille de sécurité informatique. On distingue deux types d'exploit (Exploit distant et Exploit local)

5.3.4. Rootkit

Un rootkit est un ensemble de programmes permettant d'installer sur un système des logiciels malveillants et de les rendre difficilement détectables.

Un rootkit fournit un accès administrateur à un ordinateur à l'insu de l'utilisateur en exploitant une porte dérobée.

5.Les différents types d'attaques

5.4. Malveillance Web

Les malveillances web regroupent les malveillances informatiques intentionnelles ciblant surtout le web et l'internet.

5.4.1. Cookies

Un cookie est un fichier texte disposé sur le disques dur local par un serveur Web. Il contient les informations d'identification, et ne peut pas être exécuté comme un programme, ni propager de virus.

En lui-même, un cookie ne peut nuire à un ordinateur, car il ne contient pas et ne peut contenir de code. Toutefois, un cookie peut contribuer à ce que des actions malveillantes interviennent sur le système sur lequel il est hébergé. Étant un simple fichier texte, il est aussi vulnérable et peut être lu par d'autres applications.

5.Les différents types d'attaques

5.4.2. Injection de Code

Une injection de consiste à injecter du code afin de détourner l'utilisation normale d'un programme dans le but d'exécuter un code ou une commande arbitraire. Elle peut prendre de multiples formes :

- Injection XSS (Cross Site Scripting).
- Injection SQL .
- Injection LDAP .
- Injection Xpath.

6.Les Techniques d'attaque

Plusieurs techniques d'attaques existent, nous allons nous focaliser dans ce qui suit sur les principales techniques informatiques :

6.1. Attaques de mots de passe

Une attaque par mot de passe consiste à essayer de trouver le mot de passe permettant l'accès à un compte, système ou programme, ...

6.2. Attaques de déni de service

Une attaque de déni de service (DoS, Denial of Service en anglais) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources informatiques. En général, les attaques de DoS sont à l'encontre des serveurs, afin qu'ils ne puissent être utilisés et consultés.

6.Les Techniques d'attaque

6.3. Attaques d'usurpation d'identité

L'usurpation d'identité est une technique qui consiste à se faire passer pour une entité qu'on n'est pas (protocole, application, site Web, ...). Elle peut prendre diverses formes difficiles à détecter. En général, l'attaquant n'essaie plus de tromper directement l'utilisateur mais plutôt les logiciels et les procédures automatisées du système d'exploitation.

Les techniques d'usurpation d'identité sont :

- L'usurpation d'adresse IP (spoofing IP)
- Détournement DNS (DNS spoofing)
- ARP Spoofing

6.Les Techniques d'attaque

6.4. Attaques du Man-in-the-Middle

L'attaque de l'homme au milieu (ou attaques de l'intercepteur), parfois notée MITM, est une technique d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.

La plupart des attaques de type "man in the middle" consistent à écouter le réseau à l'aide d'un sniffer.

6.5. Attaques de débordement de tampon

Débordement de tampon (buffer overflow) est une technique qui consiste à exécuter du code arbitraire par un programme en lui envoyant plus de données qu'il n'est censé en recevoir.

6.6. Attaques par injection XSS

Une attaque par injection XSS (Cross Site Scripting) est une attaque d'injection de code exécutée coté client d'une application web.

6.Les Techniques d'attaque

6.7. Attaques par failles matérielles

Les failles matérielles sont rares mais elles peuvent s'avérer très dangereuse. Ce type d'attaques consistent à exploiter les vulnérabilités des divers équipement et périphériques matériels tels que : les routeurs, les serveurs, les Bluetooth, les équipements sans fils (Wi-Fi), les processeurs (failles des techniques de virtualisation), les lecteurs d'empreinte digitale et reconnaissance faciale...

6.8. Attaques d'ingénierie sociale

L'ingénierie sociale permet parfois de pallier à l'absence de faille et d'extirper des informations de l'utilisateur d'un ordinateur sans que ce dernier n'ait conscience d'ouvrir son PC à une personne non désirée.

7. Mécanismes de protection

1. **Antivirus**
2. **Pare-feu (Firewall)**
3. **Cryptage (Chiffrement)**
4. **Réseau privé virtuel (VPN)**
5. **Système de détection d'intrusion (IDS)**

7.1. Antivirus

• Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (ex. les virus informatique).

• Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteurs de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc.

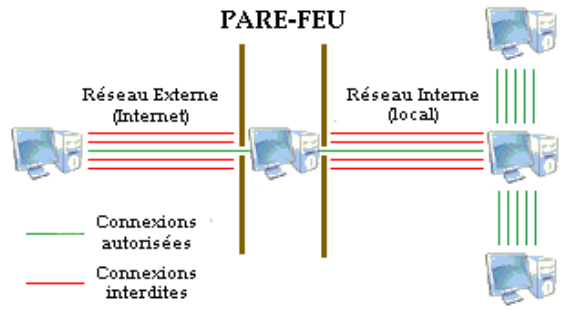
• Parmi les méthodes utilisées :

➢ Les principaux antivirus se concentrent sur des fichiers et comparent alors la signature virale du virus aux codes à vérifier. La base des signatures doit donc être très régulièrement mise à jour sur le site de l'éditeur.

➢ 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 ou modifier/supprimer des fichiers système, l'antivirus détectera ce comportement suspect et en avisera l'utilisateur qui choisira les mesures à suivre.

7.2. Pare-feu (Firewall)

• Un pare-feu (firewall en anglais), est un système physique (matériel) ou logique (logiciel) servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3, 4 et 7 du modèle OSI.



• Il s'agit donc d'une machine (machine spécifique dans le cas d'un firewall matériel ou d'un ordinateur sécurisé hébergeant une application particulière de pare-feu) comportant au minimum deux interfaces réseau :

➢ Une interface pour le réseau à protéger (réseau interne).

➢ Une interface pour le réseau externe.

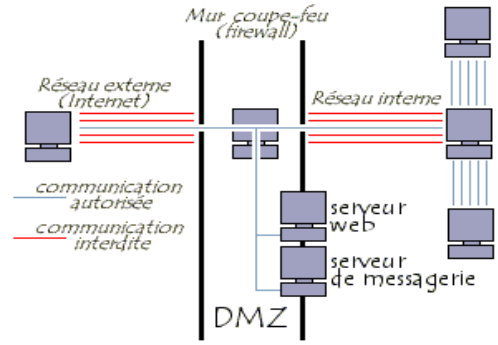
• Le pare-feu représente ainsi généralement dans les entreprises un dispositif à l'entrée du réseau qui permet de protéger le réseau interne d'éventuelles intrusions en provenance des réseaux externes (souvent internet).

Sécurité informatique : Introduction à la sécurité

• **Zone Démilitarisée (DMZ)**

- Lorsque certaines machines du réseau interne ont besoin d'être accessible de l'extérieur (par exemple pour un serveur web, un serveur de messagerie, etc.) il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise.

- On parle ainsi de zone démilitarisé (DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public.



39

Sécurité informatique : Mécanismes de protection

• **Fonctionnement d'un système pare-feu**

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

➢ D'autoriser la connexion (allow).

➢ De bloquer la connexion (deny).

➢ De rejeter la demande de connexion sans avertir l'émetteur (drop).

- L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité.

- On distingue habituellement deux types de politiques de sécurité permettant :

➢ Soit d'autoriser uniquement les communications ayant été explicitement autorisées.

➢ Soit d'empêcher les échanges qui ont été explicitement interdits.

40

Sécurité informatique : Mécanismes de protection

• **Le filtrage de paquets simple (Stateless)**

- Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « stateless packet filtering »). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

- Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice.
- Adresse IP de la machine réceptrice.
- Type de paquet (TCP, UDP, etc.).
- Numéros de port (port source et port destination).
- Flag.

41

Sécurité informatique : Introduction à la sécurité

- Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web).

- La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).

- Exemple de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

42

7.3. Cryptage (Chiffrement)

• Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement.

• Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre.

• La cryptologie est essentiellement basée sur l'arithmétique : Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique), puis ensuite de faire des calculs sur ces chiffres pour :

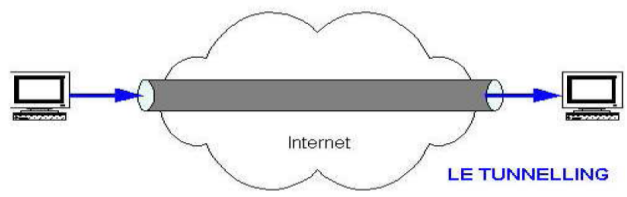
➢ D'une part les modifier de telle façon à les rendre incompréhensibles.

➢ Faire en sorte que le destinataire saura les déchiffrer.

7.4. Réseau privé virtuel (VPN)

• Dans les réseaux informatiques, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet).

• Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.



7.5. Système de détection d'intrusion (IDS)

• Même si l'intrus parvient à franchir les barrières de protection (coupe-feu, système d'authentification, etc.), il est encore possible de l'arrêter avant qu'il n'attaque. Les outils de détection d'intrusion décèlent tout comportement anormal ou trafic suspect.

• Un IDS (Intrusion Detection System) est un système informatique, composé généralement de logiciel et éventuellement de matériel, dont le rôle est la détection d'intrusions.

• C'est un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

• Il existe deux grandes familles distinctes d'IDS : les N-IDS et les H-IDS.

• **Les N-IDS (Network Based Intrusion Detection System)**

- Ils assurent la sécurité au niveau du réseau.

- Un N-IDS nécessite un matériel dédié et constitue un système capable de contrôler les paquets circulant sur un ou plusieurs lien(s) réseau dans le but de découvrir si un acte malveillant ou anormal a lieu.

- Le N-IDS place une ou plusieurs cartes d'interface réseau du système dédié en mode promiscuité (promiscuous mode), elles sont alors en mode « furtif » afin qu'elles n'aient pas d'adresse IP. Elles n'ont pas non plus de pile de protocole attachée. Il est fréquent de trouver plusieurs IDS sur les différentes parties du réseau et en particulier de placer une sonde à l'extérieur du réseau afin d'étudier les tentatives d'attaques ainsi qu'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu ou bien menée depuis l'intérieur.

• **Les H-IDS (Host Based Intrusion Detection System)**

- Ils assurent la sécurité au niveau des hôtes.

- Le H-IDS réside sur un hôte particulier et la gamme de ces logiciels couvre donc une grande partie des systèmes d'exploitation tels que Windows, Solaris, Linux, HP-UX, Aix, etc.

- Le H-IDS se comporte comme un démon ou un service standard sur un système hôte. Traditionnellement, le H-IDS analyse des informations particulières dans les journaux de logs (syslogs, messages, lastlog, wtmp,…) et aussi capture les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (Déni de Services, Backdoors, chevaux de troie, tentatives d'accès non autorisés, exécution de codes malicieux, …).

• **IPS (Intrusion Prevention System)**

- L'IPS est un Système de Prévention/Protection contre les intrusions et non plus seulement de reconnaissance et de signalisation des intrusions comme la plupart des IDS le sont. La principale différence entre un IDS (réseau) et un IPS (réseau) tient principalement en 2 caractéristiques :

➢ Le positionnement en coupure sur le réseau de l'IPS et non plus seulement en écoute sur le réseau pour l'IDS (traditionnellement positionné comme un sniffer sur le réseau).

➢ La possibilité de bloquer immédiatement les intrusions et ce quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce, ce qui induit que l'IPS est constitué en natif d'une technique de filtrage de paquets et de moyens de blocage (drop connection, drop offending packets, block intruder, …).