Les attaques :

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant des systèmes et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glâner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

Types d'attaques

Les attaques peuvent à première vue être classées en 2 grandes catégories :

- **les attaques passives** : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.
- **les attaques actives :** consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables (permettant ainsi une réponse adéquate).

Il est ainsi possible de catégoriser les risques de la manière suivante :

- **Accès physique** : il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :
    - Coupure de l'électricité
    - Extinction manuelle de l'ordinateur
    - Vandalisme
    - Ouverture du boîtier de l'ordinateur et vol de disque dur
    - Ecoute du trafic sur le réseau
- **Interception de communications** :
    - Vol de session (*session hijacking*)
    - Usurpation d'identité
    - Détournement ou altération de messages
- **Dénis de service** : il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
    - Exploitation de faiblesses des protocoles TCP/IP
    - Exploitation de vulnérabilité des logiciels serveurs
- **Intrusions** :
    - Balayage de ports
    - Elévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l'application. Les attaques par **débordement de tampon** (en anglais *buffer overflow*) utilisent ce principe.
    - Maliciels (virus, vers et chevaux de Troie
- **Ingénierie sociale** : Dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! En effet c'est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brêche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique ou en exécutant une pièce jointe. Ainsi, aucun dispositif de protection ne peut protéger l'utilisateur contre les arnaques, seuls bon sens, raison et un peu d'information sur les différentes pratiques peuvent lui éviter de tomber dans le piège !
- **Trappes** : il s'agit d'une porte dérobée (en anglais *backdoor*) dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.

Pour autant, les erreurs de programmation contenues dans les programmes sont habituellement corrigées assez rapidement par leur concepteur dès lors que la vulnérabilité a été publiée. Il appartient alors aux administrateurs (ou utilisateurs personnels avertis) de se tenir informé des mises à jour des programmes qu'ils utilisent afin de limiter les risques d'attaques.

D'autre part il existe un certain nombre de dispositifs (pare-feu, systèmes de détection d'intrusions, antivirus) permettant d'ajouter un niveau de sécurisation supplémentaire.

1. Qu'est que la sécurité ?

Faire de la sécurité sur un réseau consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible.

2. Pourquoi les systèmes sont vulnérables ?

- La sécurité est chère et difficile. Les organisations n'ont pas de budget pour ça.
- La sécurité ne peut être sûre à 100%, elle est même souvent inefficace.
- La politique de sécurité est complexe et basée sur des jugements humains.
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité.
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence.
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes (errare humanum est !).
- Il n'existe pas d'infrastructure pour les clefs et autres éléments de cryptographie.
- L'état interdit la cryptographie dans certains cas (exportation, par exemple) dans certains pays, ce qui empêche le cryptage systématique au niveau du système d'exploitation.

3. Buts de la sécurité réseau

Le but de la sécurité du réseau est de permettre la disponibilité, l'intégrité et la confidentialité :

– **La disponibilité :** signifie que les informations et les services sont accessibles et fonctionnels lorsque nécessaire. Si les systèmes ne sont pas disponibles, les deux autres points n'ont plus vraiment d'importance.

– **L'intégrité :** signifie que l'information ou le logiciel est complet, exact et authentique. L'objectif est d'empêcher tout processus ou personne non autorisée d'apporter une quelconque modification, intentionnelle ou volontaire.

Dans le cas d'une intégrité réseau, il s'agit de s'assurer que le message reçu est bien celui qui a été envoyé. Son contenu doit être intégral et non modifié.

– La confidentialité : empêche des informations sensibles d'être publié sans votre consentement ou d'être interceptée sous forme intelligible.

4. Les méthodes fondamentales de sécurisation

Les mécanismes de sécurité des réseaux informatique sont très variés mais ils reposent tous sur trois méthodes fondamentales : le chiffrement, le filtrage et les méthodes physiques.

4.1 Méthodes physiques

Nous appellerons méthodes physiques les méthodes qui ne reposent pas sur l'aspect logiciel. Il s'agit de la façon de protéger le site du réseau local (contrôle d'accès, éventuellement biométrique, gardiennage,...), de protéger la ligne spécialisée entre deux sites (pour empêcher le reniflage), et ainsi de suite.

4.2 Le chiffrement

4.2.1 Le principe du chiffrement

Le problème.- Supposons qu'un expéditeur veut envoyer un message à un destinataire. Cet expéditeur veut envoyer le message de manière sûre : il veut s'assurer qu'aucune oreille indiscrète ou oeil indiscret ne puisse s'informer du message.

La solution du chiffrement.- Le message originel à envoyer est appelé message en clair ou texte en clair (plain text en anglais).

Le chiffrement (ou cryptage) du message originel consiste à le traduire en un message incompréhensible. Le résultat de ce processus de chiffrement est appelé texte chiffré (cipher text en anglais), message codé ou cryptogramme.

Le déchiffrement (ou décryptage) consiste à traduire le message chiffré en message originel.

Le système de chiffrement est la méthode qui permet le chiffrement et de le déchiffrement.

Exemple.- L'un des premiers systèmes de chiffrement est le chiffre de Jules César, dans lequel chaque caractère du texte en clair est remplacé par celui qui se trouve trois places plus loin dans l'alphabet modulo 26 ('A' est remplacé par 'D', 'B' par 'E', ..., 'W' par 'Z', 'X' par 'A',...).

Vocabulaire.- L'art et la science de trouver des méthodes de chiffrement est appelée cryptographie, ce qui signifie hh écriture secrète ii au sens étymologique, pratiquée par des cryptographes.

L'art et la science d'essai de décryptage des messages chiffrés sans connaître le système de chiffrement et la clé utilisés est appelée la cryptanalyse, pratiquée par les cryptanalystes. La branche des mathématiques qui traite de la cryptographie et de la cryptanalyse s'appelle la cryptologie, la science du chiffrement, pratiquée par des cryptologues.

Il existe une très longue histoire des méthodes de cryptage, chaque méthode ayant été déjouée à un certain moment.

Remarque. en réalité, la protection s'applique aussi à l'image, à la voix, à des vidéos et à d'autres types de données.

D'un point de vue informatique, on le message en clair et le message codé sont des suites de bits.

4.2.2 Clés

Les processus de chiffrement reposent à la fois sur un algorithme (la méthode de chiffrement), utilisé de manière identique quel que soit le message à traiter, et sur des paramètres, appelé une clé (key en anglais). Un algorithme identique associé à différentes clés produit différents cryptogrammes à partir du même message en clair. Les méthodes de chiffrement sont peu nombreuses, si bien qu'il est impossible de les garder secrètes. Par conséquent, c'est la clé qui doit être confidentielle.

Exemple.- Par exemple pour la méthode du chiffre de Jules César, la clé peut être le décalage de lettres dans l'alphabet.

Modélisation.- On a :

cipher = encrypt(plain, key)

où encrypt() est la fonction de cryptage (encryption en anglais), ou plus exactement :

cipher = encryptALG(plain, key)

pour indiquer que le cryptage dépend de la méthode de cryptage ALG.

La fonction encrypt() doit être récursive (au sens de calculable sur ordinateur) et doit posséder une fonction réciproque également récursive pour qu'on puisse retrouver le texte en clair à partir du texte codé et de la clé :

plain = decryptALG(cipher, key)

On parle de fonction de décryptage (decryption en anglais).

4.2.3. Les types de chiffrement

Il existe deux grandes techniques de chiffrements, qui se basent sur des principes différents pour parvenir à leurs fins :

- Le chiffrement dit "symétrique", qui utilise la même clé pour chiffrer et déchiffrer les messages. Cela correspond à l'analogie du cadenas que nous avons faite : il n'existe qu'une seule clé pouvant ouvrir le cadenas, et il faut la transmettre (ou en transmettre une copie) au destinataire pour qu'il puisse l'ouvrir.

- Le chiffrement dit "asymétrique", qui quant à lui utilise non pas une clé, mais deux ! Une clé pour chiffrer un message, et une autre pour le déchiffrer

4.3. Traduction d'adresse et filtrage

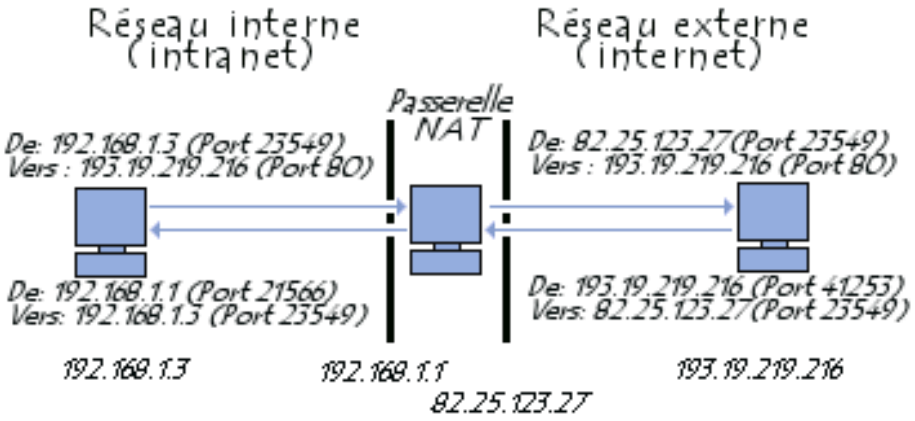
4.3.1 Traduction d'adresse en anglais *Network Address Translation* noté **NAT**)

Principe : Le mécanisme de translation d'adresses (en anglais *Network Address Translation* noté NAT) a été mis au point afin de répondre à la pénurie (manque) d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).

En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.

Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion

à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.



4.3.2. Les types de translation :

A.Translation statique

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple *192.168.0.1*) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.
La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où *n* adresses IP routables sont nécessaires pour connecter *n* machines du réseau interne.

B. Translation dynamique

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé.
Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP. C'est la raison pour laquelle le terme de « mascarade IP » (en anglais *IP masquerading*) est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.

4.3.3 Le filtrage

Lorsqu'on s'est aperçu que le service NAT a pour conséquence de renforcer la sécurité des réseaux, on a généralisé le principe sous la forme du filtrage.

Filtrage des ports.- Une première étape consiste à écarter tout paquet entrant sur le réseau local pour accéder à certains services (donc dont les ports correspondent à certains ports bien connus, comme ceux correspondants à Telent, FTP ou SMTP) ou, le plus souvent, à tout port (bien connu) sauf ceux

explicitement autorisés. La machine, en général la passerelle, chargée de ce filtrage est appelée pare-feu (firewall en anglais) de filtrage de segments.

On a généralisé de même pour les paquets sortants.

Filtrage des adresses IP.- On peut de même filtrer les adresses IP entrantes ou sortantes, grâce à un pare-feu de filtrage de paquets.

4.4. Serveur proxy

Un serveur proxy est un paquetage logiciel et/ou matériel qui permet de mettre en cache des pages Web. Il s'agit en général d'un ordinateur du réseau local à deux interfaces réseau : l'une servant à l'accès Internet, l'autre menant au réseau local. Le serveur proxy traite les requêtes Web des ordinateurs du réseau local : lorsqu'un ordinateur du réseau local émet une requête HTTP, la requête est récupérée par le serveur proxy, le serveur cherche si la page est déjà présente dans le cache (ce qui élimine le temps du chargement) et sinon est retransmise avec l'adresse publique du proxy.

La mise en cache est divisée en deux groupes : avec une mise en cache active, le serveur proxy récupère les documents dont il pense qu'ils pourront être demandés par les clients ; la mise en cache passive attend l'arrivée d'une requête avant de récupérer le document, après quoi le serveur décide si les données doivent être mises en cache.

Les serveurs proxy, à l'origine utilisés pour accélérer la récupération de documents ou pour faire face au manque d'adresses IP publiques (comme pour les serveurs NAT), sont également utilisés pour sécuriser les réseaux informatiques car la requête semble provenir du serveur, la destination n'ayant aucunement conscience du réseau situé derrière le proxy.

5 Panorama de quelques solutions

La sécurité des réseaux informatique est un domaine très actif. Plusieurs solutions ont été apportées. Énumérons quelques-unes de ces solutions, sans entrer dans le détail. Il est traditionnel de classifier les solutions suivant la couche à laquelle elle s'adresse, en commençant par la couche la plus élevée.

5.1 Sécurité de la couche d'application

Intérêts et inconvénients.- Un mécanisme de sécurité au niveau de la couche d'application procure une sécurité point à point entre une application s'exécutant sur un hôte via le réseau jusqu'à l'application sur un autre hôte.

Quelques exemples.- Il existe plusieurs essais de tels mécanismes de sécurité. Citons-en un largement utilisé et un autre maintenant presqu'abandonné.

– PGP (pour Pretty Good Privacy) est un produit utilisé pour la confidentialité et la signature numérique des messages électroniques, créé en 1991 par Phil Zimmermann. Il procure une sécurité

point à point pour le transport de fichiers de l'expéditeur au destinataire, et peut également être utilisé pour chiffrer les fichiers.

– S-HTTP (pour Secure Hyper Text Transport Protocol) a été conçu pour offrir une sécurité aux applications fondées sur le web. Il étend HTTP en ajoutant des balises pour des transactions chiffrées et fiables. Le serveur S-HTTP négocie avec le client le type de chiffrement utilisé. S-HTTP n'exige pas que les clients possèdent des certificats de clé publique, car il utilise des clès symétriques, transmises à l'avance à l'aide d'une communication hors-bande.

S-HTTP n'est pas largement utilisé, HTTPS reposant sur SSL l'ayant détrôné.

5.2 Sécurité de la couche de transport

Intérêts et inconvénients.- De nombreux mécanismes de sécurité au niveau de la couche de transport demandent la modification des applications (HHTPS au lieu de HTTP, par exemple) afin d'obtenir les avantages de la sécurité. Les applications sécurisées interviennent en remplacement des applications non sécurisées par le fait que les serveurs utilisent des ports différents.

Quelques exemples.- Il existe plusieurs essais de tels mécanismes de sécurité. Citons-en trois largement utilisés.

– SSL (Secure Sockets Layer) a été conçu par Netscape (en 1994, à l'époque où son navigateur web était largement prédominant) et est largement utilisé sur Internet pour des transactions web telles que l'envoi de données de carte de crédit, avec HTTPS. En fait SSL est plus général et peut également être utilisé pour d'autres protocoles d'application comme Telnet, FTP, LDAP, IMAP et SMTP, mais les versions sécurisées grâce à SSL n'ont pas connu de succès.

TLS (Transport Layer Scurity) est un standard ouvert proposé à l'IETF fondé sur SSL 3.0, défini par [RFC 2246, RFC 2712, RFC 2817, RFC 2818].

SSL et TLS ne procurent la sécurité qu'à une session TCP à la fois, sur laquelle n'importe quelle quantité de données peut être envoyée en toute sécurité. Le serveur et le navigateur doivent être activés SSL ou TLS pour qu'une connexion web sécurisée puisse être établie.

– SSH (Secure SHell) est un protocole, spécifié dans un ensemble de documents de brouillon Internet, qui procure une ouverture de session à distance sécurisée, qui remplace avantageusement telnet.

– Le filtrage permet de bloquer certains segments et datagrammes sur des appareils de couche de transport. Les décisions de routage ou d'abandon sont fondées sur les règles d'une liste de contrôle d'accès (ACL pour Access Control List), dites étendues car les listes de contrôle d'accès proprement dit concernent la couche réseau.

Les options de filtrage TCP comprennent les connexions établies, les numéros de port ou plages de numéros de port, ainsi que les valeurs des types de service.

Les options de filtrage UDP s'effectuent sur les numéros de port.

5.3 Sécurité de la couche réseau

Intérêts et inconvénients.- Les mécanismes de sécurité au niveau de la couche réseau sécurisent le trafic pour toutes les applications et protocoles de transport des couches supérieures. Les applications n'ont pas à être modifiées.

Quelques exemples.- Il existe essentiellement deux tels mécanismes de sécurité largement utilisés.

– Les protocoles IPSec (IP SECurity, décrit dans [RFC 2401]) peuvent fournir le contrôle d'accès, l'authentification, l'intégrité des données et la confidentialité pour chaque paquet IP entre deux noeuds réseau (hôte ou passerelle). Aucune modification du matériel ou du logiciel réseau n'est nécessaire pour router IPSec. Les applications et les protocoles de niveau supérieur peuvent rester inchangés.

IPSec ajoute deux protocoles de sécurité à IP : AH (Authentification Header) et ESP (Encapsulating Security Payload).

IPSec est à la base des réseaux virtuels (VPN pour Virtual Private Net) qui permettent d'accéder à l'intranet de son université ou de son entreprise sur un site délocalisé.

– Le filtrage permet de bloquer certains paquets au niveau des routeurs ou autres appareils de couche réseau. Les décisions de routage ou d'abandon sont fondées sur les règles d'une liste de contrôle d'accès.

5.4 Sécurité de la couche d'accès

La sécurité pour la couche d'accès est effectuée entre deux points, par exemple sur une ligne louée ou un circuit virtuel permanent. Des périphériques matériels dédiés sont situés à chaque extrémité du lien pour effectuer le chiffrement et le déchiffrement. Cette solution n'est pas applicable à de grands intér-réseaux puisque les paquets ne peuvent pas être routés sous leur forme chiffrée.

Ces mécanismes sont surtout susceptibles d'être utilisés par les militaires et les organisations financières comme les banques.