# INTRODUCTION

# A LA SECURITE DES RESEAUX

# OBJECTIFS de la SECURITE des DONNEES
(relativement à des personnes non autorisées)

Confidentielles-ne doivent pas être lues
Permanentes-ne doivent pas être altérées
Sûres- (changements détectés)
Mais les données doivent être accessibles aux personnes autorisées à :
lire, éditer, ajouter, supprimer
tout cela à travers Internet..
Interconnexion des syst. info. via des réseaux a accru la dépendance des organisations et individus/infos gérées et communiquées sur ces syst.
Ceci a conduit à une conscience accrue du besoin de protéger données et ressources des divulgations, de garantir l'authenticité de ces données et messages et de prémunir les syst. contre des attaques menées depuis les réseaux .
Importance  croissante de la sécurité des réseaux et de la cryptographie.

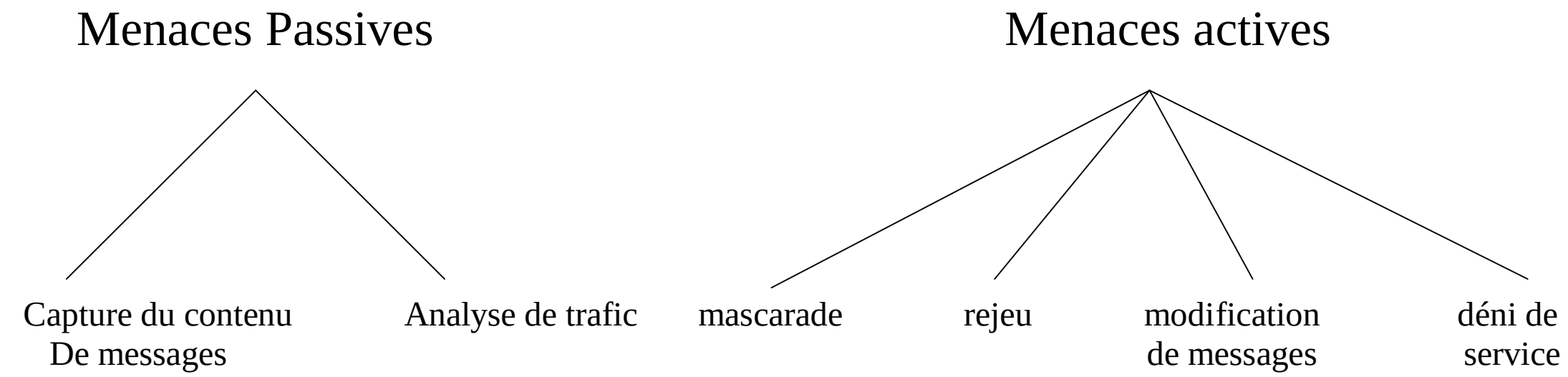
# ATTAQUES, SERVICES, MECANISMES

**Attaque de sécurité** : toute action qui compromet la sécurité de l'information possédée par une organisation

**Mécanisme de sécurité** : mécanisme conçu pour détecter, prévenir ou rattraper une attaque de sécurité.

**Service de sécurité** : service qui améliore la sécurité des systèmes informatiques et des transferts d'information d'une organisation. Ces services sont conçus pour contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité

# MENACES DE SECURITE ACTIVES ET PASSIVES



# SERVICES DE BASE EN SECURITE

**Confidentialité** protection contre la ‘lecture’ non autorisée par un tiers, coffre-fort, pli cacheté

**Authentification** assurance de l’identité d’une personne, d’un objet, CNI, passeport

**Intégrité** garantie de non modification par un tiers, document manuscrit : simple

**Non-répudiation** pour que l’émetteur ne puisse pas nier l’envoi, et que le récepteur ne puisse pas nier la réception. Transactions financières – commerciales.

**C ontrôle d’accès** autorisation ou non d’accès à des objets

**Disponibilité** attaque peut entraîner la perte ou la réduction de la disponibilité

# VIRUS, VERS, CHEVAUX DE TROIE

Virus : code (inclus dans un programme) qui se recopie lui-même dans d'autres programmes
Ver : programme se dupliquant lui-même et envoyant des copies à travers le réseau (courriels ou documents joints)
Cheval de Troie : des instructions dans un programme utile par ailleurs qui peut être la cause de mauvaises choses (envoyer votre mot de passe à un attaquant sur le net).
Bombe logique (antérieure aux virus et aux vers) : code incorporé dans des programmes légitimes et qui s'active pour 'exploser' quand un événement a lieu (date,..)
Trappes (portes dérobées) Point d'entrée secret 'écrit dans un code' (permettait de mettre au point et évaluer des programmes quand il y a un bug par exemple) qui peut autoriser des utilisateurs illégitimes

# Connexion Internet : attention danger

Fonctionnement des protocoles réseaux dans les deux sens : si vous êtes connecté à Internet, l'Internet est connecté à votre station.

Accès réseaux de votre connexion = portes ouvertes pour le piratage :

- intrusion avec récupération des droits du super utilisateur
- installation d'entrées cachées (s'introduire incognito sur la station).
- Installation d'un sniffer (écoute réseau, récupère noms utilisateurs + mots de passe associés)
- installation d'outils d'attaque pour pirater d'autres sites
- installation d'un ftp anonyme pour déposer des données illicites.

Tentatives d'intrusions régulières et journalières, par des outils 'scanners' qui vont balayer un réseau, sous-réseau à la recherche de stations vulnérables

Facile de récupérer librement sur Internet des outils de piratage.

Sécurité informatique : l'utilisateur est un acteur principal.

# Causes principales d'intrusions - Conséquences

- Non application des correctifs (patch), voie d'entrée 'su' à distance.
- Pauvreté des mots de passe
- Applications anciennes souvent ouvertes et non sécurisées. Sur des PC, versions d'antivirus obsolètes et bases de sign. non MAJ.
- Chercheurs se connectant de l'étranger et se faisant sniffer password.

Conséquences : Attaques de plus en plus destructrices :

- Disques durs inutilisables
- Destruction de données, de courriers ; vols de thèses, de brevets.
- Des labo ont servi pour mener des 'attaques par rebonds' vers des cibles externes ou des 'attaques détournées'.

But de l'intrusion : recherche d'infos sensibles d'infos sur d'autres sites
Sabotage de serveurs en les invalidant par des attaques DOS (Denial of Service) ou DDOS (Distributed …). : de + en + fréquent.
D'où, perte de temps et Pb de responsabilité . Droits et devoirs de l'util

# Minimum côté utilisateur

‘Perdez’ un peu de temps avant et non après.

- MAJ de votre windows
- Avoir un antivirus récent, MAJ de la base de sign. régulièrement

- avoir absolument un pare-feu (Firewall) personnel, filtrer les n° de port d’accès : telnet, ftp, le courrier, etc.
- utiliser ces connexions distantes sécurisées cryptées : SSH, SSF
- prendre un mot de passe non trivial
- pas d’infos confidentielles sur votre disque, ne pas en transmettre sur le réseau à moins d’utiliser le cryptage et les protocoles sécurisés
- ne pas récupérer n’importe quoi n’importe où, au moins toujours passer le prog (même récupéré en courrier attaché) à un anti-virus récent et mis à jour régulièrement

- Facile de récupérer lors de votre connexion des infos sur votre syst, vos logiciels, le degré de sécu, sur la non-appli des patchs.
- Se connecter sur Internet n'est pas anonyme : lors d'un passage sur un site, vous laissez une adresse IP, un nom de login, une adresse ) tout sur les cookies, www.privacy.com est aussi édifiant
- logiciels gratuits contiennent des espiongiciels . Conclusion : fermez votre PC aux intrus (comme votre porte à clé)