Université Abou Bakr Belkaid
Faculté des sciences
Département d'Informatique

Sécurité Informatique

Chapitre 1: Notions Fondamentales

Présenté par Mme Labraoui N.

Master 1 Réseaux et systèmes distribués

2019-2020

Introduction

- La sécurité est un enjeu majeur des technologies numériques modernes:
  - Infrastructures de télécommunication (GSM, GPRS, UMTS),
  - réseaux sans fils (Bluetooth, WiFi, WiMax),
  - Internet,
  - Systèmes d'information,
  - routeurs, ordinateurs, téléphones, décodeurs de télévision, assistants numériques,
  - systèmes d'exploitation, applications informatiques
- toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration.

Introduction

- Virus informatiques, actes de malveillance interne ou externe, failles de sécurité, espionnage industriel, tous ces dangers constituent la préoccupation majeure des responsables informatiques des entreprises.
- Cette inquiétude se manifeste aussi chez les utilisateurs et parvient même à troubler la confiance des citoyens dans leur relation avec les technologies numériques.

- La sécurité des réseaux et des systèmes est une discipline en pleine évolution

La typologie des réseaux et des systèmes

- Le monde numérique des réseaux et des systèmes comprend :

1. les réseaux informatiques : les réseaux locaux d'entreprises, les réseaux de vidéo surveillance sur IP, Internet, les réseaux sans fil (WiMax, WiFi, Bluetooth), les réseaux passifs d'étiquettes intelligentes (RFId) ;
2. les réseaux de télécoms : les réseaux satellites, les réseaux de localisation GPS ou Galiléo, les réseaux téléphoniques, les réseaux d'opérateurs de téléphonie mobile (GSM, GPRS, EDGE, UMTS) ;
3. les réseaux de diffusion de télévision (TNT, câble) et de radio
4. les SI de l'État, des institutions, des entreprises, des banques, des organisations, des réseaux à domicile (réseau domestique), de gestion des infrastructures critiques et du patrimoine numérique naissant des familles et des individus.

Les concepts et la démarche de la sécurité

- La démarche traditionnelle de la sécurité consiste à cloisonner les ressources (réseaux et serveurs) et les informations (programmes et données) en fonction de leur sensibilité et de leur domaine d'application, dans le respect de la réglementation.
  - Objectifs de la sécurité
  - La politique de sécurité
  - Les fonctions de sécurité

Les objectifs de la sécurité

- La sécurité numérique brigue trois objectifs :

1. la confidentialité,
2. l'intégrité
3. la disponibilité des ressources et des informations des réseaux et des systèmes.

- S'ajoutent à ces 3 objectifs d'autres objectifs tels que: authenticité, non-répudiation et le contrôle d'accès. (qu'on verra dans la suite de cette présentation)

Les objectifs de la sécurité
la confidentialité

- la confidentialité, vise à assurer que seuls les sujets (les personnes, les machines ou les logiciels) autorisés aient accès aux ressources et aux informations auxquelles ils ont droit.
- La confidentialité a pour objectif d'empêcher que des informations secrètes soient divulguées à des sujets non autorisés.
- L'objectif des attaques sur la confidentialité est d'extorquer des informations ;

Les objectifs de la sécurité
l'intégrité

- l'intégrité vise à assurer que les ressources et les informations ne soient pas corrompues, altérées ou détruites par des sujets non autorisés.
- L'objectif des attaques sur l'intégrité est de changer, d'ajouter ou de supprimer des informations ou des ressources

Les objectifs de la sécurité
la disponibilité

- la disponibilité vise à assurer que le système soit bien prêt à l'emploi, que les ressources et les informations soient en quelque sorte consommables, que les ressources ne soient pas saturées, que les informations, les services soient accessibles et que l'accès au système par des sujets non autorisés soit prohibé.
- L'objectif des attaques sur la disponibilité est de rendre le système inexploitable ou inutilisable.
- **La cryptologie permet de remplir largement les deux premiers objectifs en confidentialité et en intégrité.**
- **Malheureusement, il n'existe pas de modèles pour parvenir entièrement à la finalité de disponibilité**

La politique de sécurité

- Pour atteindre ces objectifs de sécurité, il est nécessaire de mettre en œuvre une politique de sécurité.
- Cette politique désigne l'ensemble des lois et des consignes aux fins de protéger les ressources et les informations contre tout préjudice à leur confidentialité, leur intégrité et leur disponibilité
- La politique exhibe, dans sa rédaction sous forme de règles, des sujets et des objets et précise les activités et opérations autorisées et interdites.

Étapes types dans l'établissement d 'une politique d e sécurité

1. **Identification des vulnérabilités**
   - En mode fonctionnement normal : (définir tous les points faibles)
   - En cas d'apparition de défaillances: un système fragilisé est en général vulnérable : c'est dans un de ces moments intermédiaires qu'une intrusion peut le plus facilement réussir
2. ***Évaluation des probabilités associées à chacune des menaces***
3. ***Évaluation du coût d'une intrusion réussie***
4. ***Choix des contre mesures***
5. ***Évaluation des coûts des contre mesure***
6. ***Décision***

Les fonctions de sécurité

- La politique de sécurité utilise un catalogue de fonctions de sécurité, parmi lesquelles on peut trouver :
  1. l'identification des sujets
  2. l'authentification
  3. l'intimité numérique
  4. la traçabilité
  5. l'audit du système,
  6. l'imputabilité des actions
  7. l'autorisation des actions
  8. le contrôle d'accès
  9. la protection des contenus
  10. La gestion de sécurité

1 l'identification des sujets

- l'identification des sujets, des objets et des opérations effectuées par ces sujets sur ces objets.
- Il s'agit de donner un nom à une personne, à une carte graphique, à un document, à un paquet IP.
- Un sujet qui n'a pas de nom est anonyme. Dans ce cas, le sujet ne peut être tenu responsable d'une action fautive.
- Un sujet peut avoir un pseudonyme (un alias) : il cache alors son vrai nom, mais reste responsable des actions qu'il pourrait exécuter sous son faux nom ;

2 l'authentification

- l'authentification, c'est-à-dire la preuve de l'identité de ces entités ou de ces opérations.
- Il s'agit d'un processus incorruptible pour garantir que le sujet est bien celui qu'il prétend être, pour garantir que l'objet est bien celui que l'entité responsable nomme ou bien que l'opération est bien celle qu'elle doit être

3 l'intimité numérique

- l'intimité numérique est une fonction qui consiste à abriter l'identité d'une entité et ses activités, en masquant son observation.
- Une manière de satisfaire cette intimité est de rester anonyme, mais un anonymat sévère peut à son tour devenir un danger pour autrui, se traduire par une irresponsabilité des actes et affaiblir la sécurité de l'ensemble du système

4 la traçabilité

- la traçabilité, c'est-à-dire une fonction qui consiste à repérer l'histoire des entités (ou des fractions d'entités).
- La traçabilité peut localiser par intermittence la position d'un sujet ou d'un objet, peut dater des transactions, peut noter des renseignements sur des situations, le tout avec des attributs de sécurité.
- Cette fonction s'avère irremplaçable pour contrôler un objet, pour pister un suspect ou pour reconstituer un scénario lors d'une enquête ou d'une perquisition informatique

5 l'audit du système

- i.e l'observation, l'enregistrement, l'analyse et la compréhension des événements importants ou anormaux qui vont concourir à reconstituer le fil de son histoire, après une panne ou d'une attaque.
- on enregistre, dans les différents dispositifs de sécurité, des journaux infalsifiables qui seront des témoins de confiance chargés d'interpréter la trame des opérations et d'imputer la responsabilité d'une erreur ou d'un acte malveillant à son initiateur.
- Le cybercriminel s'efforce de dissimuler les traces de son passage en tentant de détériorer ces fichiers d'audit.
- L'auditabilité est une fonction qui consiste à pouvoir récupérer des preuves numériques incontestables, en cas de perquisition des données ou d'examen ultérieur des activités

6 l'imputabilité

- l'imputabilité des actions d'un sujet sur des objets, en relation avec sa responsabilité. Par exemple, la non-répudiation.
- est une fonction qui permet de garantir qu'une communication ou une transaction ne peut être niée, ni à l'émission, ni à la destination par ses responsables

7 l'autorisation des actions

- l'autorisation des actions par un sujet sur des objets. Les droits spécifiques et les privilèges des sujets sont définis par cette fonction.

8 le contrôle d'accès

- le contrôle d'accès, c'est-à-dire la restriction d'accès aux ressources et aux informations, aux seuls sujets qui sont autorisés.
- Il s'agit, par exemple, de filtrer les flux entrant et sortant dans un périmètre selon des règles définies

9 la protection des contenus

- la protection des contenus, i.e la confidentialité et l'intégrité des informations des utilisateurs.
- Il s'agit de cacher la signification des informations aux sujets non autorisés, en utilisant des primitives cryptographiques.

10 la gestion de la sécurité

- la gestion de la sécurité, c'est-à-dire la gestion du cycle de vie de toutes les fonctions précédentes, essentiellement la configuration et la protection de ces fonctions de sécurité.
- L'objectif de la gestion de la sécurité est d'établir et de maintenir un état de sécurité conforme à la politique en vigueur.

Statistiques sur la sécurité et sur le coût de l'insécurité

- Il existe de nos jours 20 000 attaques réussies (sur un ou plusieurs sites) par mois dans le monde.
- Cependant la cartographie et le volume de la délinquance dans le cyberespace sont mal connus car la plupart des infractions commises ne sont pas portées à la connaissance des autorités.
- la **métrologie des attaques** est un domaine de recherche pour mesurer, en toute intelligibilité, la dangerosité d'un site, d'un système ou d'un réseau et pour jauger ou annoncer une «météorologie des attaques » sur un réseau.

Statistiques sur la sécurité et sur le coût de l'insécurité

- On comptait environ 70 000 virus en 2004.
- L'augmentation est d'environ 1000 par mois, mais il n'existe environ que 10 000 virus actifs en permanence.
- Pendant le pic d'une infection, 10 % des mails de l'Internet sont infectés.
- En 2005, le spam comprend quelque 20 milliards de messages par jour à l'échelle mondiale.
- les fraudes sur les cartes bancaires et sur les téléphones sont finalement plus importantes, car elles se caractérisent par des pertes financières directes, alors que les virus et les spams n'engendrent en général qu'indirectement des coûts financiers qui se comptent toutefois par milliards d'euros par an, à l'échelle mondiale.
- On peut estimer le coût des dommages directs de la cybercriminalité dans les entreprises à **1 milliard d'euros** par an, mais le coût global de l'insécurité numérique culmine plutôt vers **50 milliards d'euros** par an.

Statistiques sur la sécurité et sur le coût de l'insécurité

- Le marché mondial de la sécurité des systèmes d'information est de l'ordre de 20 milliards d'euros,
- mais le marché mondial de la sécurité numérique dans le cadre de la convergence avoisine 80 milliards d'euros.
- En règle générale, les dépenses de sécurité sont de l'ordre de 5% à 10 % du budget correspondant aux technologies numériques.

La typologie des attaquants

- Les pirates du numérique appartiennent à des catégories très hétéroclites. Ce sont :
  1. **des cyberterroristes** qui exploiteront bientôt le côté virtuel du réseau pour harceler et atteindre des cibles stratégiques, dans l'intention de déstabiliser les États et terroriser les populations ;
  2. **des cybercriminels** qui cultivent la dimension de communication du réseau pour gagner de l'argent (vol, extorsion) de manière frauduleuse et pour fertiliser leur propre réseau de diffusion : délinquance, mafia, casinos, blanchiment d'argent, narcotique, contrefaçon, proxénétisme, pédophilie, racisme, sectes en tout genre ;
  3. **des *hackers*, *des cyberpunks*** *: sur un mode ludique, ces amateurs (souvent informaticiens adolescents) se* lancent des défis, publient les découvertes de failles de sécurité sur les OS et les protocoles, jouent sur le réseau à déverrouiller des accès, transgressant la législation à leurs risques et périls
  4. **des organisations privées ou gouvernementales** qui commanditent des interventions peu recommandables ou délictueuses : intelligence économique sur Internet, surveillance, écoutes, interceptions, infractions envers des concurrents ;
  5. **des utilisateurs standard** qui ont des pratiques illégales comme le téléchargement de fichiers musicaux ou l'utilisation illégale de logiciels.

Etude des risques

- Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi.
- Il est nécessaire de réaliser une analyse de risques en prenant soin d'identifier les problèmes potentiels avec les solutions et les coûts associés.
- L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque.
- On obtient ainsi la liste de ce qui doit être protégé.

Etude des risques

- Voici quelques éléments pouvant servir de base à une étude de risques:
  - Quelle est la valeur des équipements, logiciels et surtout des informations ?
  - Quel est le coût et le délai de remplacement?
  - Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseaux (programmes d'analyse de paquets, logs…)
  - Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la societé?

Quels sont les risques ?

Evaluation des risques liées à l'utilisation de l'informatique

Il importe de mesurer ces risques :

- en fonction de la probabilité ou de la fréquence de leurs survenances ;
- en mesurant leurs effets possibles.

- **le traitement informatique en cours échoue** : il suffit de le relancer, éventuellement par une autre méthode si on craint que la cause ne réapparaisse ;
- **l'incident est bloquant** et on doit procéder à une réparation ou une correction avant de poursuivre le travail entrepris.
- **données irrémédiablement perdues ou altérées,** ce qui les rend inexploitables ;
- **données ou traitements durablement indisponibles,** pouvant entraîner l'arrêt d'une production ou d'un service ;
- **divulgation d'informations confidentielles ou erronées pouvant profiter à des sociétés** concurrentes ou nuire à l'image de l'entreprise ;
- déclenchement d'actions pouvant provoquer des **accidents physiques ou induire des drames humains.**

Les risques humains

Ce sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés.

Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

- la **maladresse :** commettre des erreurs : exécuter un traitement non souhaité, effacer
- **l'inconscience et l'ignorance :** introduire des programmes malveillants sans le savoir (par exemple lors de la réception de courrier).

  De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils font courir aux systèmes qu'ils utilisent.
- la **malveillance :** impossible d'ignorer les différents problèmes de virus et de vers ces dernières années (beaucoup de couverture médiatique).

  Certains utilisateurs peuvent volontairement mettre en péril le système d'information, en y introduisant en connaissance de cause des virus (en connectant par exemple un ordinateur portable sur un réseau d'entreprise), ou en introduisant volontairement de mauvaises informations dans une base de données.

  Il est facile pour un informaticien d'ajouter délibérément des fonctions cachées lui permettant, directement ou avec l'aide de complices, de détourner à son profit de l'information ou de l'argent.

  *On parle alors de la « **cyber-criminalité** ».*

Les risques humains

- **l'ingénierie sociale (**social engineering) est une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins (publicitaires par exemple).

Elle consiste à :

- se faire passer pour quelqu'un que l'on est pas (en général un administrateur)
- demander des informations personnelles (nom de connexion, mot de passe, données confidentielles, etc.) en inventant un quelconque prétexte .
- Elle peut se faire soit au moyen d'une simple communication téléphonique, soit par mail, soit en se déplaçant directement sur place.
- l'espionnage : surtout industriel, emploie les même moyens, ainsi que bien d'autres, pour obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, clients et prospects, etc.

Les risques matériels

- Ils sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels.
- Incidents liés au matériel : la plupart des composants électroniques, produits en grandes séries, peuvent comporter des défauts. (tomber en panne).

  Certaines de ces pannes sont assez difficiles à déceler car intermittentes ou rares.

  Parfois, elles relèvent d'une erreur de conception (une des toutes premières générations du processeur Pentium d'Intel pouvait produire, dans certaines circonstances, des erreurs de calcul) ;
- Incidents liés au logiciel : plus fréquents ; Les systèmes d'exploitation et les programmes sont de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent l'effort conjoint de dizaines, de centaines, voire de milliers de programmeurs. Ces programmeurs peuvent faire des erreurs de manière individuellement ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité.
- Incidents liés à l'environnement : les machines électroniques et les réseaux de communication sont sensibles aux variations de température ou d'humidité (tout particulièrement en cas d'incendie ou d'inondation) ainsi qu'aux champs électriques et magnétiques.

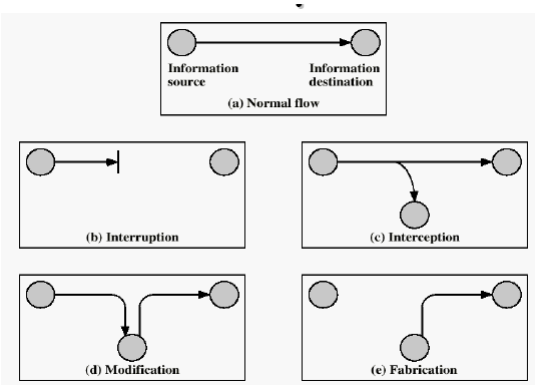
Les précautions à prendre

- **redondance des matériels** : la probabilité ou la fréquence de pannes d'un équipement est représentée par un nombre très faible.
- En doublant ou en triplant (ou plus) un équipement, on divise le risque total par la probabilité de pannes simultanées.
- Le résultat est donc un nombre beaucoup plus faible et la fiabilité est plus grande.
- **dispersion des sites** : un accident (incendie, tempête, tremblement de terre, attentat, etc.) a très peu de chance de se produire simultanément en plusieurs endroits distants.
- **procédures de contrôle indépendants** : ils permettent bien souvent de déceler les anomalies avant qu'elles ne produisent des effets dévastateurs.

  Il est possible de réaliser des audits de sécurité.

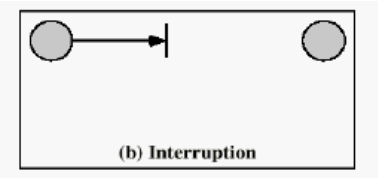
Les d'attaques de sécurité

- Les attaques portées à la sécurité d'un ordinateur ou d'un réseau sont mieux caractérisées en considérant le système en tant que fournisseur d'information.
- Il existe quatre catégorie d'attaques : interruption, interception, modification, fabrication.



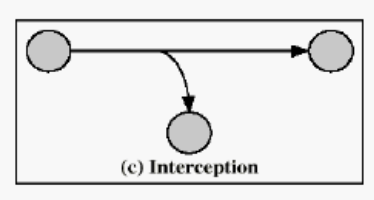
Attaques de sécurité : interruption

- Un atout du système est détruit ou devient indisponible ou inutilisable.
- C'est une attaque portée à la disponibilité.
- La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples.



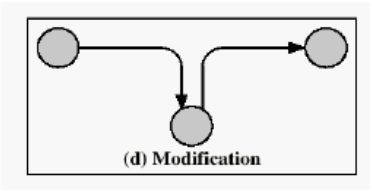
Attaques de sécurité : interception

- Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la confidentialité.
- Il peut s'agir d'une personne, d'un programme ou d'un ordinateur.
- Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples.



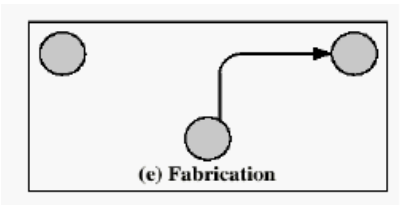
Attaques de sécurité : modification

- Une tierce partie non autorisée obtient accès à un atout et le modifie de façon (presque) indétectable.
- Il s'agit d'une attaque portée à l'intégrité.
- Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.



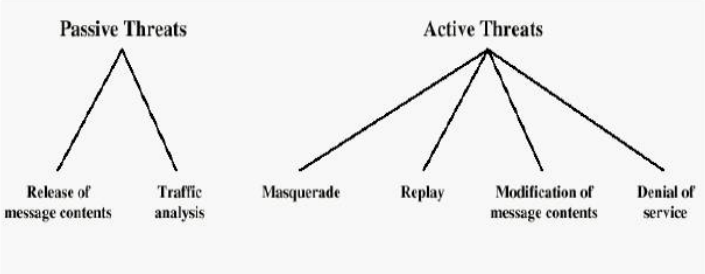
Attaques de sécurité : fabrication

- Une tierce partie non autorisée insère des contrefaçons dans le
- système.
- C'est une attaque portée à l'authenticité.
- Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier.



Attaques passives et attaques actives

- Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives.



Attaques passives (1/2)

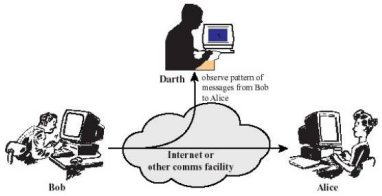
- Écoutes indiscrètes ou surveillance de transmissions sont des attaques de nature passive.
- Le but de l'adversaire est d'obtenir une information qui a été transmise.
- Ces attaques passives sont la capture du contenu d'un message et l'analyse de trafic.

1. **La capture du contenu** de messages est facilement compréhensible. Une conversation téléphonique, un courrier électronique ou un fichier transféré peuvent contenir une information sensible ou confidentielle.

Attaques passives (2/2)

2. **l'analyse de trafic:** (2 ème attaque passive), est plus subtile.

- Supposons qu'un moyen de masquer le contenu des messages ou des informations soit à disposition (par exemple, un système de chiffrement), de sorte que les adversaires, même en cas de capture, ne pourront en extraire l'information contenue. Cependant l'adversaire pourra être en mesure d'observer le motif de ces messages, déterminer l'origine et l'identité des systèmes en cours de communication, et observer la fréquence et la longueur des messages échangés.
- Cette information peut être utile pour deviner la nature de la communication.
- **Les attaques passives sont très difficiles à détecter car elles ne causent aucune altération des données.**

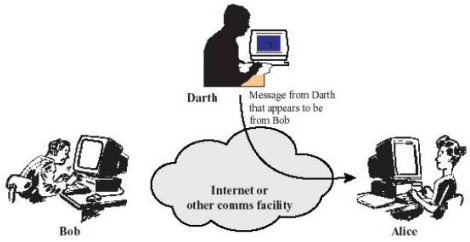


Attaques actives (1/4)

- Ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux ; elles peuvent être subdivisées en 4 catégories: mascarade, rejeu, modification de messages et déni de service.

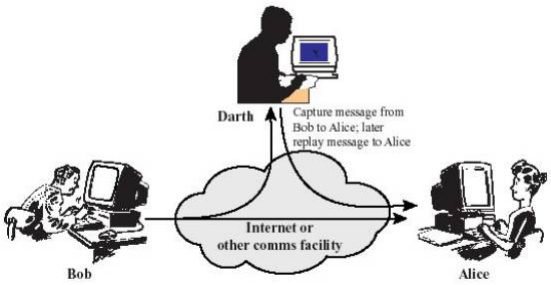
1. **Une mascarade** a lieu lorsqu'une entité prétend être une autre entité. Une attaque de ce type inclut habituellement une des autres formes d'attaque active.

   Par exemple, des séquences d'authentification peuvent être capturées et rejouées, permettant ainsi à une entité autorisée munie de peu de privilèges d'en obtenir d'autres en usurpant une identité possédant ces privilèges.



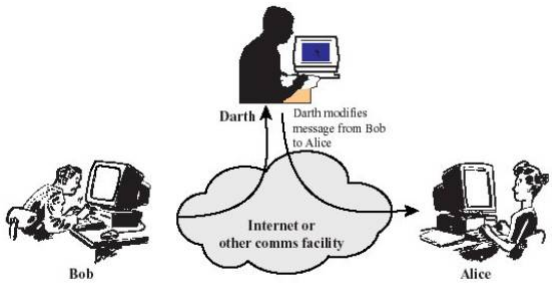
Attaques actives (2/4)

2. **Le rejeu** implique la capture passive de données et leur retransmission ultérieure en vue de produire un effet non autorisé.



Attaques actives (3/4)

3. **La modification de messages (« man in the middle »)**
   signifie que certaines portions d'un message légitime sont altérées ou que les messages sont retardés ou réorganisés. Par exemple, le message " autoriser **X** à lire le fichier confidentiel comptes " est modifié en " autoriser **Y** à lire le fichier confidentiel comptes ".



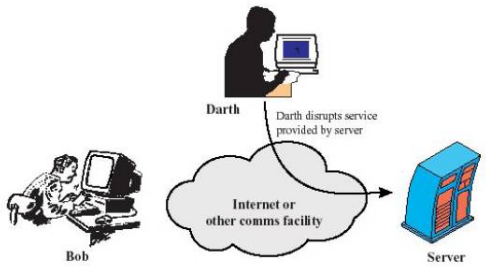
Attaques actives (4/4)

3. **Le déni de service (DoS)**

   empêche l'utilisation normale ou la gestion de fonctionnalités de communication. Cette attaque peut avoir une cible spécifique ;

   par exemple, une entité peut supprimer tous les messages dirigés vers une destination particulière.

   Une autre forme de refus de service est la perturbation d'un réseau dans son intégralité, soit en mettant hors service le réseau, soit en le surchargeant de messages afin de dégrader ses performances.



Typologie des attaques informatiques

Bombe logique

- est une partie d'un programme malveillant (virus, cheval de Troie, etc.) qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou encore que certaines conditions soient réunies, pour déclencher des effets dévastateurs.
- Le virus Tchernobyl, qui fut l'un des virus les plus déstructeurs, avait une bombe logique qui s'est activée le 26 avril 1999, jour du treizième anniversaire de la catastrophe nucléaire de Tchernobyl.

Typologie des attaques informatiques

Cheval de Troie

- (trojan en anglais) est un programme effectuant une fonction illicite tout en donnant l'apparence d'effectuer une fonction légitime.
- La fonction illicite peut consister en la divulgation ou l'altération d'informations.
- Trojan.ByteVerify est un cheval de Troie sous forme d'une applet java. Ce cheval de Troie exploite une vulnérabilité de la machine virtuelle java de Microsoft permettant à un pirate d'exécuter du code arbitraire sur la machine infectée. Par exemple, Trojan.ByteVerify peut modifier la page d'accueil d'Internet Explorer.

Typologie des attaques informatiques

Porte dérobée

- (ou backdoor en anglais) est un moyen de contourner les mécanismes de contrôle d'accès.
- Il s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle (cheval de Troie en particulier).
- C'est donc une fonctionnalité inconnue de l'utilisateur légitime qui donne un accès secret au logiciel. Une porte dérobée a été découverte dans le SGBD interbase de Borland au début des années 2000. Il suffisait d'entrer le nom d'utilisateur " politically " et le mot de passe " correct " pour se connecter à la base de données avec les droits d'administrateur.

Typologie des attaques informatiques

Routeurs

- Portes dérobées
  - ⇨ comptes par défaut pour les fabricants
  - ⇨ tous niveaux y compris administrateur
  - ⇨ présents sur tous types de routeurs
  - ⇨ mots de passe sur l'Internet !!!

ex :

Routeurs	*Login*	*Password*
3Com	admin	synnet
3Com	manager	manager
Cisco	enable	cisco
Bay Networks	Manager	<null>

Typologie des attaques informatiques

Virus

- Un virus est un segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'une application), et qui devient ainsi un cheval de Troie.
- Puis le virus peut ensuite se propager à d'autres ordinateurs (via un réseau) à l'aide du programme légitime sur lequel il s'est greffé.
- Il peut également avoir comme effets de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté.
- PsybOt, découvert en 2009, est considéré comme étant le seul virus informatique ayant la capacité d'infecter les routeurs et modems haut-débit.

Typologie des attaques informatiques

Ver

- Un ver est un programme autonome qui se reproduit et se propage à l'insu des utilisateurs.
- Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour se dupliquer. Le ver a habituellement un objectif malicieux, par exemple :
- espionner l'ordinateur dans lequel il réside ;
- offrir une porte dérobée à des pirates informatiques ;
- détruire des données sur l'ordinateur infecté ;
- envoyer de multiples requêtes vers un serveur internet dans le but de le saturer.
- Le ver Blaster avait pour but de lancer une attaque par déni de service sur le serveur de mises à jour de Microsoft.

Typologie des attaques informatiques

le logiciel espion

- (*spyware) : fait de la collecte d'informations personnelles sur l'ordinateur d'un* utilisateur sans son autorisation.
- Ces informations sont ensuite transmises à un ordinateur tiers ;