Sécurité des réseaux informatiques

Bernard Cousin
Université de Rennes 1

Introduction

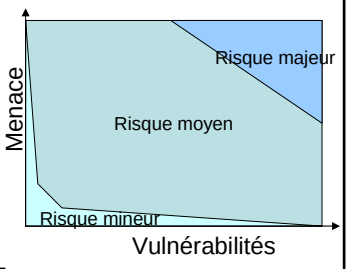
- Risques
- Attaques, services et mécanismes
- Les attaques
- Services de sécurité
- Mécanismes de défense
- Politique de sécurité
- Architectures de sécurité

Bibliographie

- Stallings, W. *Network Security Essentials, 2nd edition*. Prentice Hall, 2003
  - Un grand nombre de figures ont été extraites de ce livre
  - Support de cours inspiré de Henric Johnson (Blekinge Institute of Technology, Sweden)
- Maiwald, E. *Network Security*, Mc Graw Hill, 2001 (traduction Campus Press)

Gestion des risques

- Vulnérabilité + menace = risque
  - Menace : cible + agent + conséquence
    - Fichier source + employé + "bug"
  - Vulnérabilité : cible + agent + procédé
    - Fichier source + employé + altération (in)volontaire
- Contre-mesures
    - Exemple : Authentification + contrôle des droits de modification
  - Compromis efficacité/coût des contre-mesures
    - coût de l'incident versus coût des contre-mesures



Les objets de la sécurité

- Les informations
- Le système
- Le réseau
- Etc.

Attaques, Services and Mécanismes

- **Une Attaque :** n'importe quelle action qui compromet la sécurité des informations.
- **Mécanismes de Sécurité :** un mécanisme qui est conçu pour détecter, prévenir et lutter contre une attaque de sécurité.
- **Service de Sécurité :** un service qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité.

Attaques

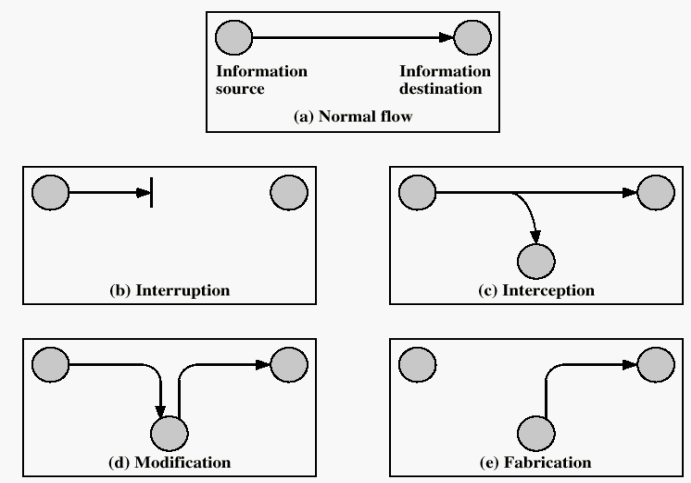


Figure 1.1 Security Threats

Buts des attaques

- **Interruption**: vise la disponibilité des informations
- **Interception**: vise la confidentialité des informations
- **Modification**: vise l'intégrité des informations
- **Fabrication**: vise l'authenticité des informations

Attaques passives ou actives

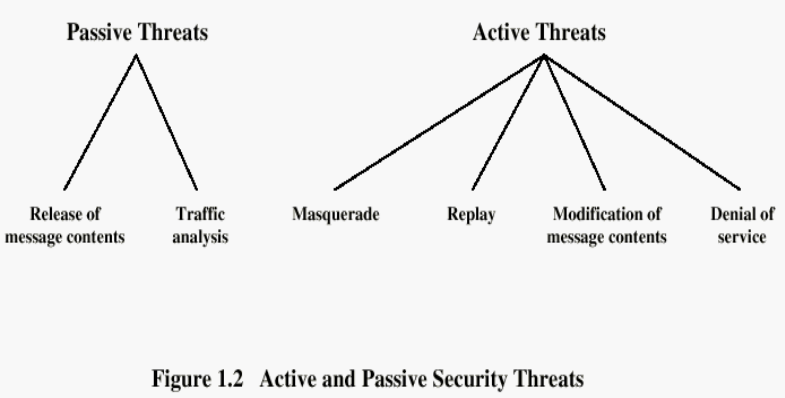
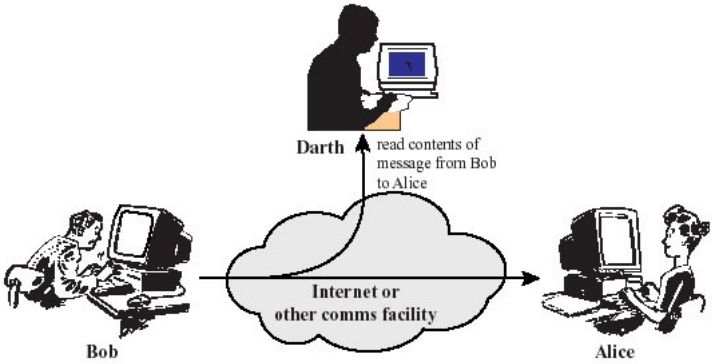
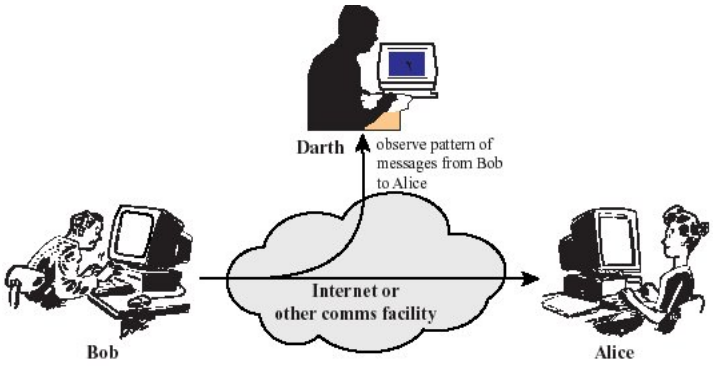


Figure 1.2 Active and Passive Security Threats

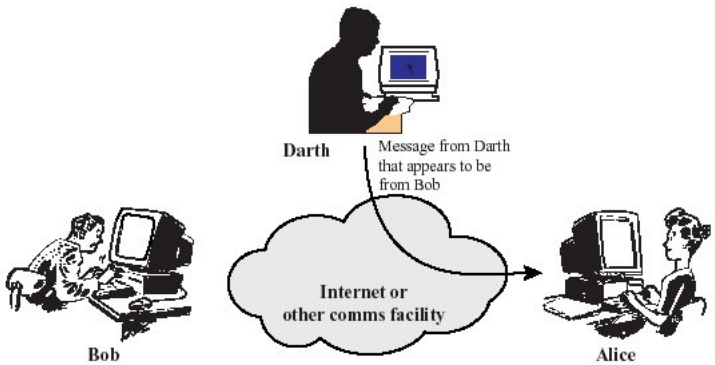
Description des attaques : capture



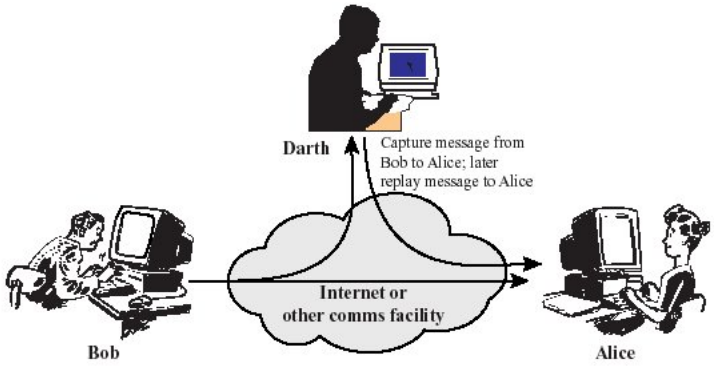
Description des attaques : analyse de trafic



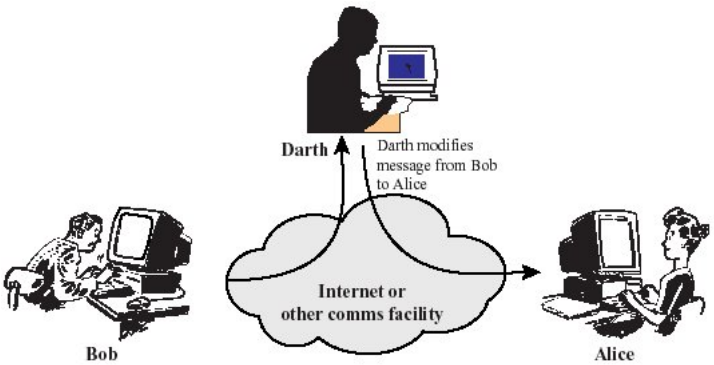
Description des attaques : masquarade



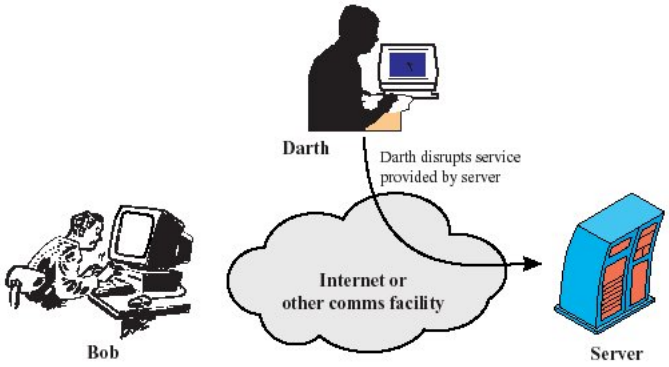
Description des attaques : rejeu



Description des attaques : modification ("man in the middle")



Description des attaques : Déni de service ("DoS")



Services de Sécurité

- **Confidentialité** : les données (et l'objet et les acteurs) de la communication ne peuvent pas être connues d'un tiers non-autorisé.
- **Authenticité** : l'identité des acteurs de la communication est vérifiée.
- **Intégrité** : les données de la communication n'ont pas été altérées.
- **Non-répudiation** : les acteurs impliqués dans la communication ne peuvent nier y avoir participer.
- **Disponibilité** : les acteurs de la communication accèdent aux données dans de bonnes conditions.

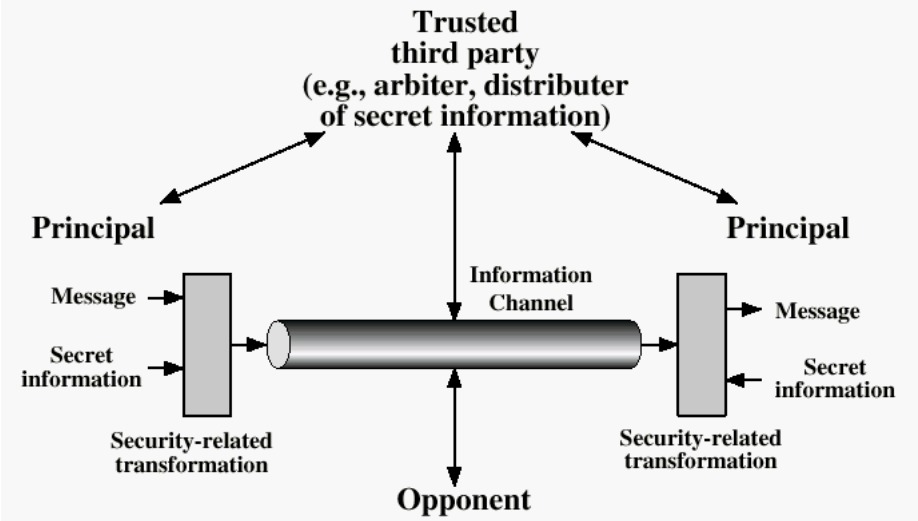


Figure 1.3 Model for Network Security

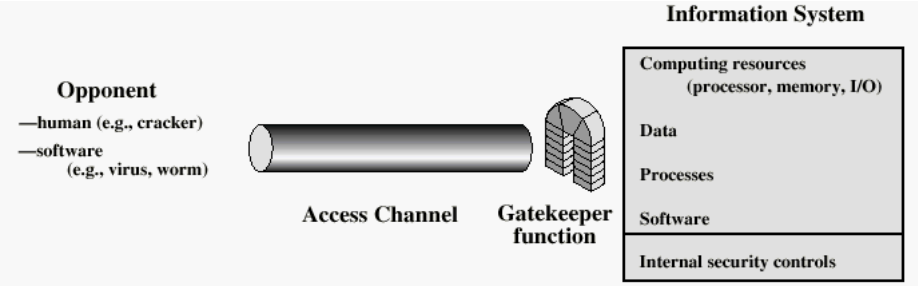


Figure 1.4 Network Access Security Model

Mécanismes de défense

- **Chiffrement** : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
- **Signature** numérique: données ajoutées pour vérifier l'intégrité ou l'origine des données.
- **Bourrage de trafic** : données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- **Notarisation** : utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- **Contrôle d'accès** : vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.

Mécanismes de défense

- **Antivirus** : logiciel censé protéger ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.
- **Le pare-feu** : un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).
- **Détection d'intrusion** : repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs.
- **Journalisation** ("logs") : Enregistrement des activités de chaque acteurs. Permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.
- **Analyse des vulnérabilité** ("security audit") : identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu.

Mécanismes de défense

- **Contrôle du routage** : sécurisation des chemins (liens et équipements d'interconnexion).
- **Contrôle d'accès aux communications** : le moyen de communication n'est utilisé que par des acteurs autorisés. Par VPN ou tunnels.
- **Horodatage** : marquage sécurisé des instants significatifs .
- **Certification** : preuve d'un fait, d'un droit accordé.
- **Distribution de clefs** : distribution sécurisée des clefs entre les entités concernées.

Mécanismes de défense

- **Authentification** : Authentifier un acteur peut se faire en utilisant une ou plusieurs de ses éléments.
  - Ce qu'il sait. Par ex. : votre mot de passe, la date anniversaire de votre grand-mère
  - Ce qu'il a. Par ex. : une carte à puce
  - Ce qu'il est. Par ex. : la biométrie (empreinte digitale, oculaire ou vocale)
  - Dans le domaine des communications, on authentifie l'émetteur du message. Si l'on considère les (deux) extrémités d'une communication il faut effectuer un double authentification
    - Par ex. pour lutter contre le "phishing"
  - L'authentification est nécessaire au bon fonctionnement des autres mécanismes.
- **La protection physique** : peut fournir une protection totale, mais qui peut être excessive. Par ex. isoler complètement son système est une solution qui peut être trop radicale.

Remarques sur la confiance

- Confiance dans la sécurité d'un système:
  - Système réparti = {système de communication, les sous-systèmes locaux}
  - Niveau de confiance d'un système = min (niveau de confiance de ses sous-systèmes)
- Dans un système sûre de confiance
  - Les mécanismes de sécurité peuvent formellement établir la confiance
  - Création d'un chaîne de confiance
    - Les amis surs de mes amis sont des amis surs
  - Problème du point de départ de la chaîne de confiance
    - L'authentification des centres de certification
  - Renforcement de la confiance, au cours des échanges
    - Graphe de confiance
  - Révocation de la confiance accordée

Remarques sur les mécanismes de sécurité

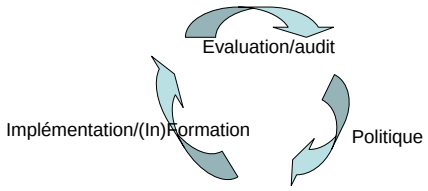
- Aucun des mécanismes de sécurité ne suffit par lui-même. Il les faut tous !

Politique de sécurité

- Une politique de sécurité ce n'est pas seulement :
  - Les paramètres de sécurité
    - longueur des clefs,
    - choix des algorithmes,
    - fréquence de changement des "passwords",
    - etc.
- Une fois une politique de sécurité définie, sa mise en oeuvre (utilisation d'outils appropriés) et sa bonne gestion (maintien de la cohérence) sont des points critiques

Le processus de sécurité

- Evaluation/audit
- Politique
- Implémentation/(In)Formation
- Evaluation …



Quelques procédures de sécurité

- Définition du domaine à protéger
- Définition de l'architecture et de la politique de sécurité
  - Equipements/Points de sécurité
  - Paramètres de sécurité
  - C-à-d mécanismes de prévention, détection et enregistrement des incidents
- Plan de réponse après incident
  - Procédure de reprise
  - Procédure pour empêcher que cela se renouvelle
    - Suppression de la vulnérabilité, ou suppression de l'attaquant
- Charte du bon comportement de l'employé
- Procédures d'intégration et de départ des employés
- Politique de mise à jour des logiciels
- Méthodologie de développement des logiciels
- Définition des responsabilités (organigramme)
- Etc.

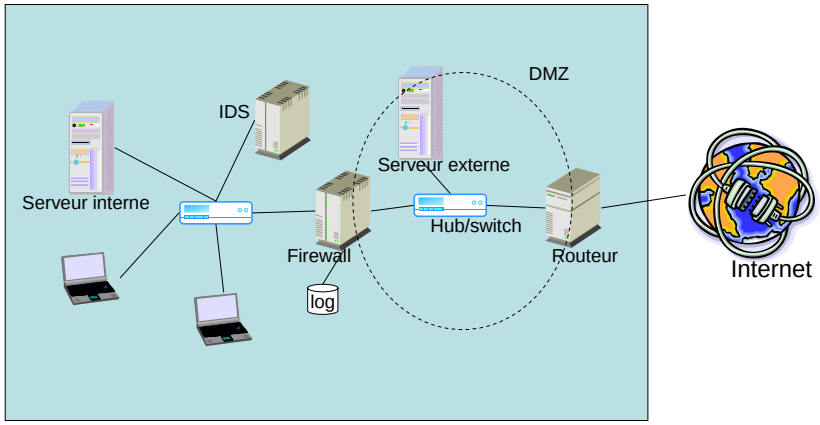
Le facteur humain

- Le facteur humain est souvent prépondérant:
  - Respect des règles de sécurité
  - Compréhension de l'utilité des règles,
  - Surcharge induit par les moyens de sécurité
- L'ingénierie sociale

Eléments d'architecture

- Pare-feu
- DMZ
- IDS
- Log
- VPN

Eléments d'architecture



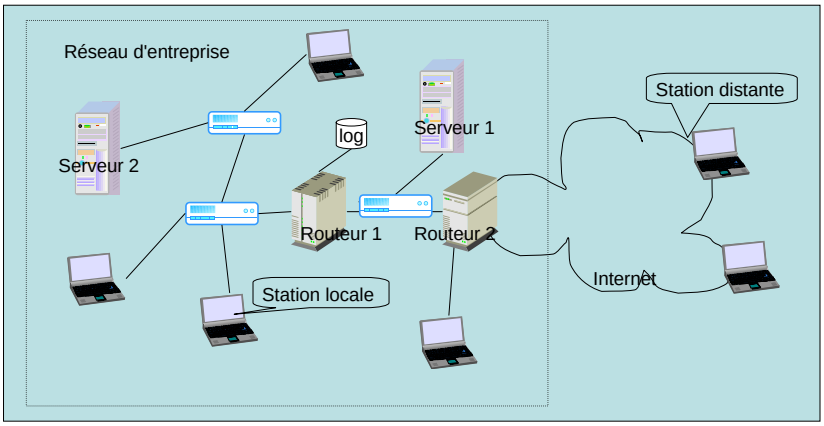
Virtual Private Network

- Seuls les agents autorisés peuvent avoir accès aux réseaux virtuels
  - Authentification des agents
  - Chiffrement des communications
- Remarques:
  - Le réseau virtuel est un moyen d'accéder à des services (extension au réseau de la notion de contrôle d'accès aux fichiers)
  - On limite délibérément la capacité d'interconnexion totale proposée par l'Internet
  - Le nombre des réseaux virtuels dépend du nombre des types d'agents (et donc des services accessibles à chaque type d'agent)

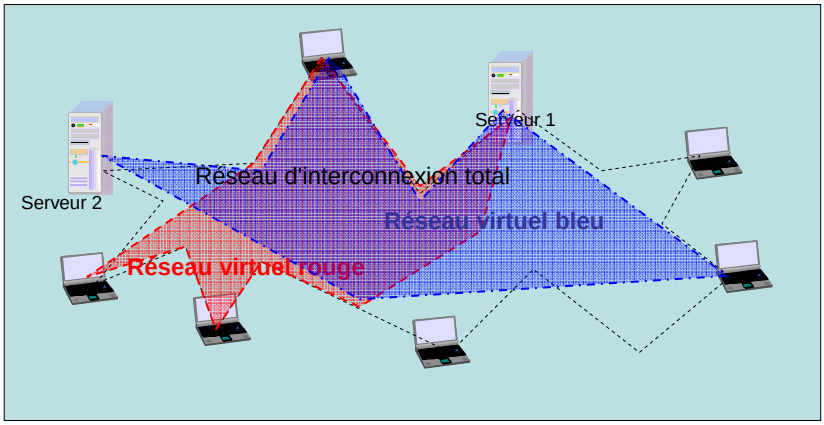
Réseau virtuel

- Il existe de nombreuses implémentations du concept de réseau virtuel :
  - Au niveau 2 : VLAN
    - Les trames Ethernet sont complétées par un VID
  - Au niveau 3 : IPsec+
    - Accompagné d'une phase d'authentification (serveur d'authentification)
    - Les paquets sont chiffrés (serveurs de sécurité)

Réseaux virtuels



Réseaux virtuels



Conclusion

- Présentation des risques (attaques), services et mécanismes de sécurité
- Introduction à la politique et architecture de sécurité