



# ISCAE

## Réseaux et Télécommunications

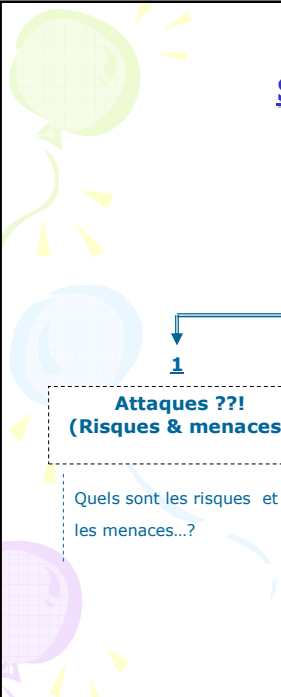
« Sécurité des réseaux »

2012 - 2013

Saadbouh O CHEIKH EL MEHDI



1



## Sécurité des réseaux

### - Introduction -

Sécurité des réseaux

1

2

3

**Attaques ??!**  
**(Risques & menaces)**

**Services de sécurité**

**Mécanismes**

Quels sont les risques et les menaces...?

Quels sont les services permettant de garantir la sécurité ? Ou augmenter son niveau ?

Quels sont les mécanismes déployés pour rendre les services de sécurité ?

2

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux - Introduction -

**Une Attaque :** toute action qui compromet la sécurité des informations.

### **Service de Sécurité :**

- Un service qui augmente la sécurité (le niveau de sécurité) dans un réseau.
- Conçu pour contrer une attaque
- Utilise un ou plusieurs mécanisme de sécurité

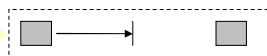
**Mécanismes de Sécurité :** un mécanisme qui est conçu pour détecter, prévenir et lutter contre une attaque de sécurité.

3

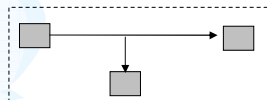
Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux - Introduction -

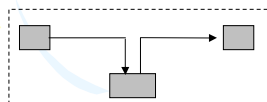
### Buts des attaques



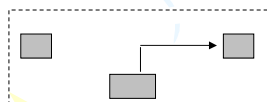
1. **Interruption** : vise la disponibilité des données



2. **Interception** : vise la confidentialité des données



3. **Modification** : vise l'intégrité des données



4. **Fabrication** : vise l'authenticité des données

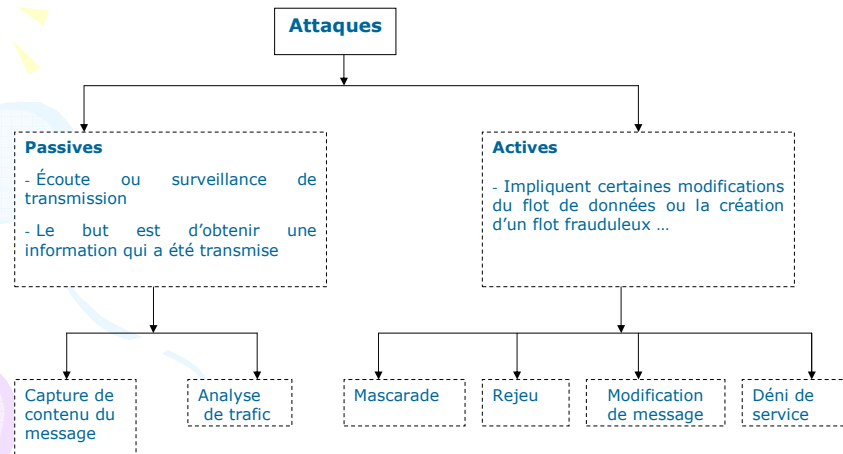
4

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux

### - Introduction -

#### Types d'attaques



5

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux

### - Introduction -

#### Types d'attaques

**Mascarade** : - une entité prétend être une autre entité  
- une attaque de ce type inclut habituellement une des autres formes d'attaques actives

**Rejeu** : implique la capture passive des données et leur retransmission ultérieure en vue de produire un effet non-autorisé

**Modification de message** : Signifie que certaines portions d'un message légitime sont altérées ou que les messages sont retardés ou réorganisés

**Déni de service** : empêche l'utilisation normale ou la gestion de fonctionnalité de communication

6

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux

### - Introduction -

#### Services de Sécurité

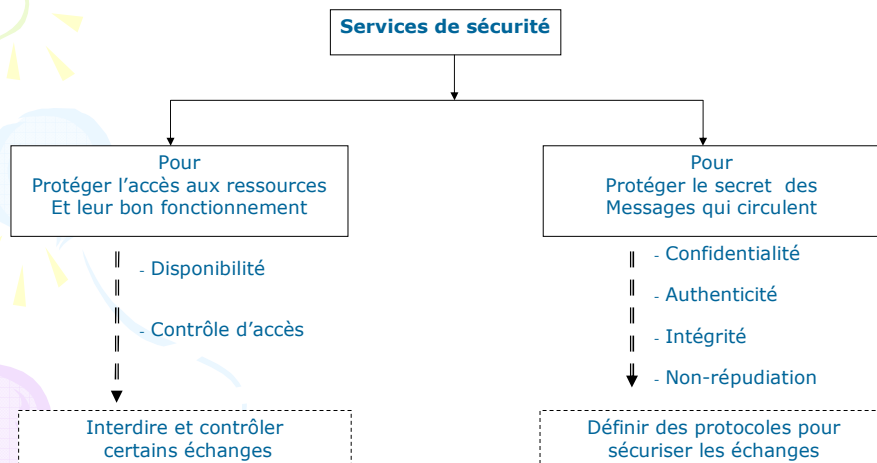
- **Confidentialité** : les données (et l'objet et les acteurs) de la communication ne peuvent pas être connues d'un tiers non-autorisé.
- **Authenticité** : l'identité des acteurs de la communication est vérifiée.
- **Intégrité** : les données de la communication n'ont pas été altérées.
- **Non-répudiation** : les acteurs impliqués dans la communication ne peuvent nier y avoir participé.
- **Disponibilité** : les acteurs de la communication accèdent aux données dans de bonnes conditions.
- **Contrôle d'accès**: le service de contrôle d'accès empêche l'utilisation non autorisée de ressource accessible par le réseau

7

## Sécurité des réseaux

### - Introduction -

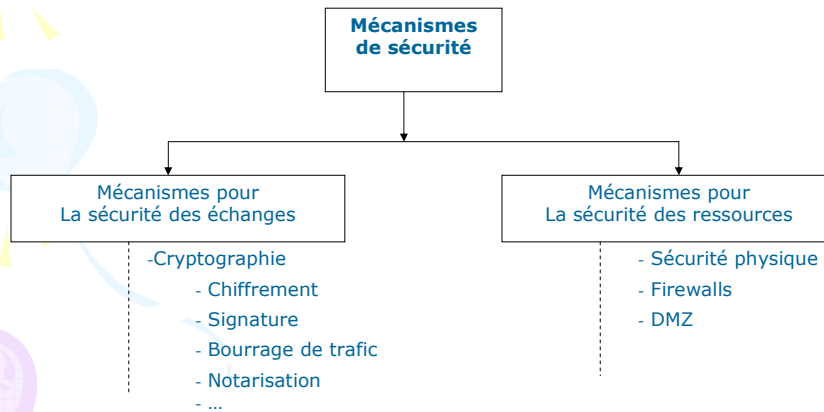
#### Services de Sécurité



8

## Sécurité des réseaux - Introduction -

### Mécanismes de Sécurité



9

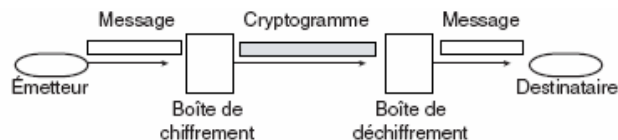
Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux - Introduction -

### Sécurité des échanges

**Cryptographie** : - deux mots crèques: **crypto**=caché et **graphie** =écrire  
- Science du **chiffrement**

**Chiffrement** : - transforme tout ou partie d'un texte dit *clair* en *cryptogramme*, message chiffré ou protégé



10

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux - Introduction -

### Sécurité des échanges

#### Chiffrement

- Le mécanisme de chiffrement émet un message  $X$  sous une forme secrète au moyen d'une clé  $K$
- L'émetteur dispose d'une fonction algorithmique  $E$ , qui, à  $X$  et  $K$ , associe  $E(K, X)$
- Le récepteur reçoit  $E(K, X)$  et le déchiffre au moyen de sa clé  $K'$  avec sa fonction algorithmique de déchiffrement  $D$ , qui à  $E(K, X)$  et  $K'$  associe  $X$ . On a alors :

$$D(K', E(K, X)) = X$$

- Les fonctions  $E$  et  $D$  peuvent être secrètes ou publiques. Il en est de même pour les clés  $K$  et  $K'$

11

## Sécurité des réseaux - Introduction -

### Sécurité des échanges

#### Chiffrement

- Une clé = chaîne de chiffre binaires (0 et 1) (i.e. un nombre ou autre)
- Un Algorithme = fonction mathématique qui va combiner la clé et le texte à crypter pour rendre ce texte illisible

#### Chiffrement symétrique

- Historiquement, les premiers algorithmes de chiffrement étaient tels que  $K = K'$  et  $D = E^{-1}$ .
- La clé  $K$ , unique, était secrète et l'algorithme du récepteur consistait à faire l'inverse de l'algorithme de l'émetteur
- Il suffisait de connaître la clé  $K$ .
- On parle alors de **chiffrement symétrique** car il n'y a qu'une clé.

12



## Sécurité des réseaux - Introduction -

### Sécurité des échanges

#### Chiffrement symétrique

- **Avantage:**

- Rapide

- **Inconvénients:**

- Il faut autant de paires de clés que de couples de correspondants
- La Non-répudiation n'est pas assurée. Mon correspondant possédant la même clé que moi, il peut fabriquer un message en usurpant mon identité
- Transmission de clé

13



## Sécurité des réseaux - Introduction -

### Sécurité des échanges

#### Chiffrement asymétrique

##### Deux clefs :

- Clé publique : Sert à chiffrer le message
- Clé privée : Sert à déchiffrer le message
- Clé publique du destinataire (diffusée largement) utilisée pour le chiffrement du « message »
- Clé privée du destinataire (confidentielle !) utilisée pour le déchiffrement du « message »

14



## Sécurité des réseaux - Introduction -

### Sécurité des échanges

#### Chiffrement asymétrique

##### Avantages :

- Pas besoin de se transmettre les clés au départ par un autre vecteur de transmission.

##### Inconvénients:

- Lenteur

15



## Sécurité des réseaux - Introduction -

### Sécurité des échanges

#### Signature numérique

- Données ajoutées pour vérifier l'intégrité ou l'origine des données.
- Consiste à utiliser un chiffrement particulier appelé chiffrement *Irréversible*
- Transforme un message (*a priori* long) en un bloc de données (de petite taille) tel qu'il est impossible de reconstruire le message à partir du bloc
- Les algorithmes utilisés sont appelés *fonction de hachage*

16





## **Sécurité des réseaux** **- Introduction -**

### **Sécurité des échanges**

#### **Bourrage de trafic**

- Données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- Simule des communications dans le but de masquer les périodes de silence et de banaliser les périodes de communication réelles
- Permet d'éviter d'attirer l'attention lors des démarrages de transmission.

17



## **Sécurité des réseaux** **- Introduction -**

### **Sécurité des échanges**

#### **Notarisation**

- Utilisation d'un tiers de confiance pour assurer certains services de sécurité
- Apporte une garantie supplémentaire: les entités font confiance à un tiers qui assure l'intégrité et atteste de l'origine, la date et la destination des données

18

## Sécurité des réseaux - Introduction -

### Sécurité des ressources

Protéger les ressources revient à contrôler les accès aux ressources protégées. Cela signifie:

- Contrôler d'où proviennent les connexions et vers où elles se dirigent
- Contrôler le type de connexion (connexion incorrecte par exemple pour rendre indisponible un service)

La sécurité des ressources se base sur des techniques réseaux (et pas cryptographiques) :

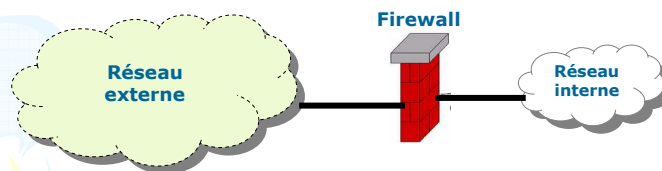
- Ajout de fonctionnalités à des protocoles
- Des équipements physiques
- Des solutions logicielles, ...

19

## Sécurité des réseaux - Introduction -

### Sécurité des ressources

#### Firewalls (Pare-Feux)



- Un domaine à protéger = réseau interne (réseau d'entreprise ou personnel)
- Protection vis à vis d'un réseau externe (en général Internet)
  - Contre des intrus susceptibles de faire des attaques

20

## Sécurité des réseaux - Introduction -

### Sécurité des ressources

#### Firewall

Un Firewall est un logiciel, un équipement réseau, ou les deux, qui permet de filtrer les messages qui circulent (entrants et sortants).

Il est situé sur une machine utilisateur ou sur une machine tenant lieu de passerelle ou de routeur donnant accès (passage obligatoire) à un ou des (sous-) réseaux.

- Le filtrage consiste à écrire un ensemble de filtres (règles).
- Si un paquet correspond à la règle, il est détruit et on garde éventuellement une trace de son passage.
- Il assure donc le contrôle d'accès pour un réseau ou une machine.

21

## Sécurité des réseaux - Introduction -

### Sécurité des ressources

#### Firewall

##### Firewall

##### Peut faire

- Être un guichet de sécurité: un point central de contrôle de sécurité plutôt que de multiples contrôles dans différents logiciels clients ou serveurs.
- Appliquer une politique de contrôle d'accès.
- Enregistrer le trafic: construire des journaux de sécurité.
- Appliquer une défense en profondeur (multiples pare-feux)

##### Ne peut pas faire

- Protéger contre les utilisateurs internes
- Protéger un réseau d'un trafic qui ne passe pas par le pare-feu (exemple de modems additionnels)
- Protéger contre les virus.
- Protéger contre des menaces imprévues (hors politique).

22

## Sécurité des réseaux - Introduction -

### Sécurité des ressources

#### Demilitarized Zone : DMZ

##### Notion de cloisonnement

- Les systèmes pare-feu permettent de définir des règles d'accès entre deux réseaux
- Or les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes :
  - Les serveurs web, ftp, messagerie, ... doivent être accessibles de l'extérieur
  - Les postes utilisateurs sur le LAN ne doivent pas l'être !
- Donc, il est nécessaire que le système de pare-feu cloisonne les différents sous-réseaux de l'entreprise

→ Cloisonnement des réseaux

23

## Sécurité des réseaux - Introduction -

### Sécurité des ressources

#### Demilitarized Zone : DMZ

##### Définition

Un sous-réseau "entre" un réseau sécurisée (intranet /réseau local) et un réseau moins, peu, voire pas, sécurisé (Internet / WAN).

Des services que l'on peut accéder depuis l'extérieur y sont déployés.

##### Utilité

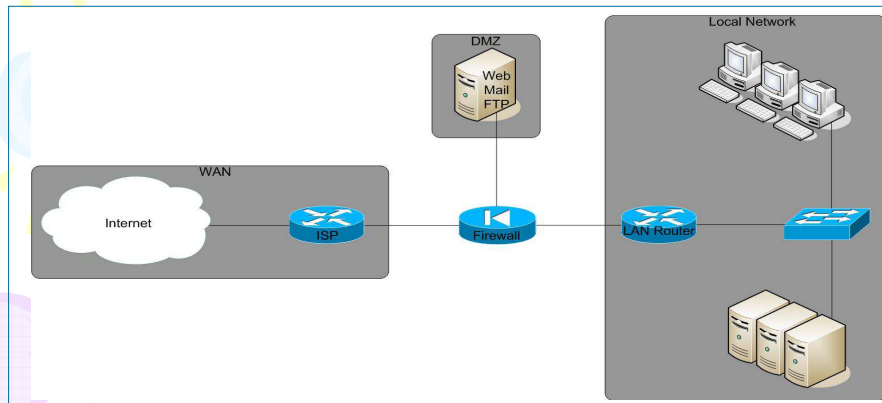
- Permettre l'accès à des ressources internes au réseau, tout en gardant la partie sécurisée à l'abri des attaques externes
- Ressources: serveur Web, Mail, FTP, DNS, ...etc.

24

## Sécurité des réseaux - Introduction -

### Sécurité des ressources

#### Demilitarized Zone : DMZ



25

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi

## Sécurité des réseaux - Introduction -

### Quelques attaques bien connues

#### Préparation d'une attaque

- Collecter des informations sur les ressources de la cible:
  - Pour les adresses IP : **ping, traceroute...**
  - Scanning de ports: plusieurs techniques (fonction **connect()**, **TCP SYN Scan**, ...)
  - Mots de passes : sniffing de paquets ...
- IP spoofing
  - Déguiser une adresse IP :
    - Éviter d'être détecté, et donc arrêté
    - Permet d'échapper au filtrage d'adresse IP

#### Parades

- Filtrer ICMP
- Détecter les interfaces en mode promiscuité (interface récupérant tous les paquets, même ceux qui ne lui sont pas adressés)
- ...etc.

26

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi



## Sécurité des réseaux - Introduction -

### Quelques attaques bien connues

#### 1. Le déni de service (DoS, Denial of Service)

- Consiste à bloquer une machine cible en lui envoyant des requêtes inutiles
- Empêche la machine de rendre le service pour lequel on l'a installée
  - inondation par des *ping* (messages *ICMP Echo Request*)
  - des messages ICMP avec beaucoup de données nécessitant la fragmentation
- **La machine cible passe son temps à répondre aux sollicitations reçues et n'a plus de disponibilité pour son propre service**

27

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi



## Sécurité des réseaux - Introduction -

### Quelques attaques bien connues

#### 2. L'inondation de requêtes d'ouverture (SYN Flooding)

- L'attaque par inondation de requêtes d'ouverture consiste à envoyer à une machine cible un grand nombre de segments avec drapeaux **SYN** mais sans jamais transmettre le troisième segment
- La machine cible réserve vainement des ressources à chaque requête d'ouverture et passe son temps à gérer les temporisateurs d'attente du troisième segment qui confirme l'ouverture

#### Rappel

Une demande d'ouverture de connexion TCP (segment avec drapeau SYN = 1) provoque une réponse avec les drapeaux SYN et ACK mis à 1 puis une attente du troisième segment avec seulement le drapeau ACK = 1

28

Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi



## Sécurité des réseaux

### - Introduction -

#### Quelques attaques bien connues

##### 3. Dissimulation d'adresse IP (IP Spoofing)

- Un pirate veut attaquer un réseau dont il connaît l'adresse IP : il usurpe l'une de ces adresses et l'utilise comme adresse source.
- Il y a toutes les chances pour que son datagramme soit considéré comme un datagramme normal du réseau
- sauf s'il se présente, venant d'Internet, à la porte d'entrée du réseau et que l'administrateur **a prévu** qu'un message avec une adresse IP d'émetteur interne ne puisse pas provenir de l'extérieur.

##### Rappel

*Le datagramme IP transporte l'adresse IP de l'émetteur et, en l'absence d'un mécanisme d'authentification de l'adresse, il est impossible de vérifier qui a émis avec cette adresse.*

29



## Sécurité des réseaux

### - Introduction -

#### Quelques attaques bien connues

##### 4. Autres attaques

Les pirates ont toujours beaucoup d'imagination:

- Utiliser un port (ouvert) proposé pour un protocole donné avec un autre protocole ce qui donne des possibilités de manipulations sur la machine cible
- Voler des sessions (*hijacking*) TCP ouvertes de l'intérieur
- Profiter des failles de sécurité sur une machine pour l'utiliser ensuite comme source et profiter des droits d'accès de celle-ci (rebond)
- Réinjecter dans le réseau des messages corrects (chiffrés, signés...) qui ont déjà été transmis (rejeu)
- Chevaux de Troie (Un Cheval de Troie - *trojan en anglais*- est un programme effectuant une fonction illicite tout en donnant l'apparence d'effectuer une fonction légitime)
- ...etc.

30