Chapitre 1 : Introductio

(sécurité et parallélisme)

Plan

- Contexte réseau
- Définitions

1. Contexte réseau

- Modèle OSI
- Internet
- Besoin de sécurité
- Paradigmes

Modèle OSI

- Couches : application, présentation, s
  transport, réseau, liaison de données
- Caractéristiques
  - transparence entre couches
  - encapsulation
- Couches réseau
  - saut à saut : réseau (IP, ARP), liaison d
    physique
  - bout en bout : transport (TCP, UDP)

Internet

- Réseau ouvert par principe
- Plusieurs millions de machines interc
- Basé sur IP
  - protocole fonctionnant en *best-effort*
  - opacité de l'adressage
    - sous la responsabilité de l'administrateur
    - adressage privé
    - translation de ports et d'adresses

Besoin de sécurité

- Utilisateur légitime
  - en général, pas compétent en sécurité
- Attaquant
  - pas de contrôle
  - peu de lois
- Fournisseur de services
  - la sécurité possède rarement un aspect

Paradigmes

- Paradigme 1 : la sécurité d'un systèm
  niveau de sécurité de sa plus faible p
- Paradigme 2 : la sécurité est un com
  entre :
  - les risques
  - le coût (financier et performance)

2. Définitions

- Types d'attaques
- Moyens d'attaques
- Services de sécurité
- Méthodes de protection

Types d'attaques

- Flux normal : A → B
- Interruption : A →
  - (attaque sur la disponibilité)
- Interception : A → B et A → X
  - (attaque sur la confidentialité)
- Modification : A → X et X → B
  - (attaque sur l'intégrité)
- Fabrication : X → B
  - (attaque sur l'autenticité)

Moyens d'attaques

- Passifs
  - obtention de messages
  - analyse du trafic
- Actifs
  - mascarade
  - rejeu
  - modification des messages
  - déni de service

Services de sécurité

- Confidentialité
- Intégrité
- Identification (connaître l'identité, *log*
- Autentification (vérifier l'identité, *pass*
- Non-répudiation (impossibilité de nier ou la réception)
- Contrôle d'accès
- Disponibilité

Méthodes de protectio

- Chiffrement
- Protections logicielles
  - système d'exploitation (droits)
- Protections matérielles
- Architecture réseau, infrastructure de
- Politiques
  - politiques de mots de passe