Licence 3

SI

Sécurité Informatique

Dr Souheila Bouam

Maître de conférences A
Université Batna-2
Département Informatique

s.bouam@univ-batna2.dz

Plan

- Rappels
- Relation Risques, Vulnérabilités et Menaces
- Objectifs de la sécurité
- Services de sécurité
- Attaques existantes
- Mécanismes de défense
- Etude de cas: IDS (Intrusion Detection Systems)
- Mécanismes supplémentaires de sécurité

Rappels

- Il n'existe pas un système informatique sécurisé à 100% sauf s'il est complètement isolé!

↪ Un système informatique accessible par plusieurs utilisateurs ou connecté à un réseau (qu'il soit local ou étendu) devient menacé.

↪ Un tel système doit être sécurisé

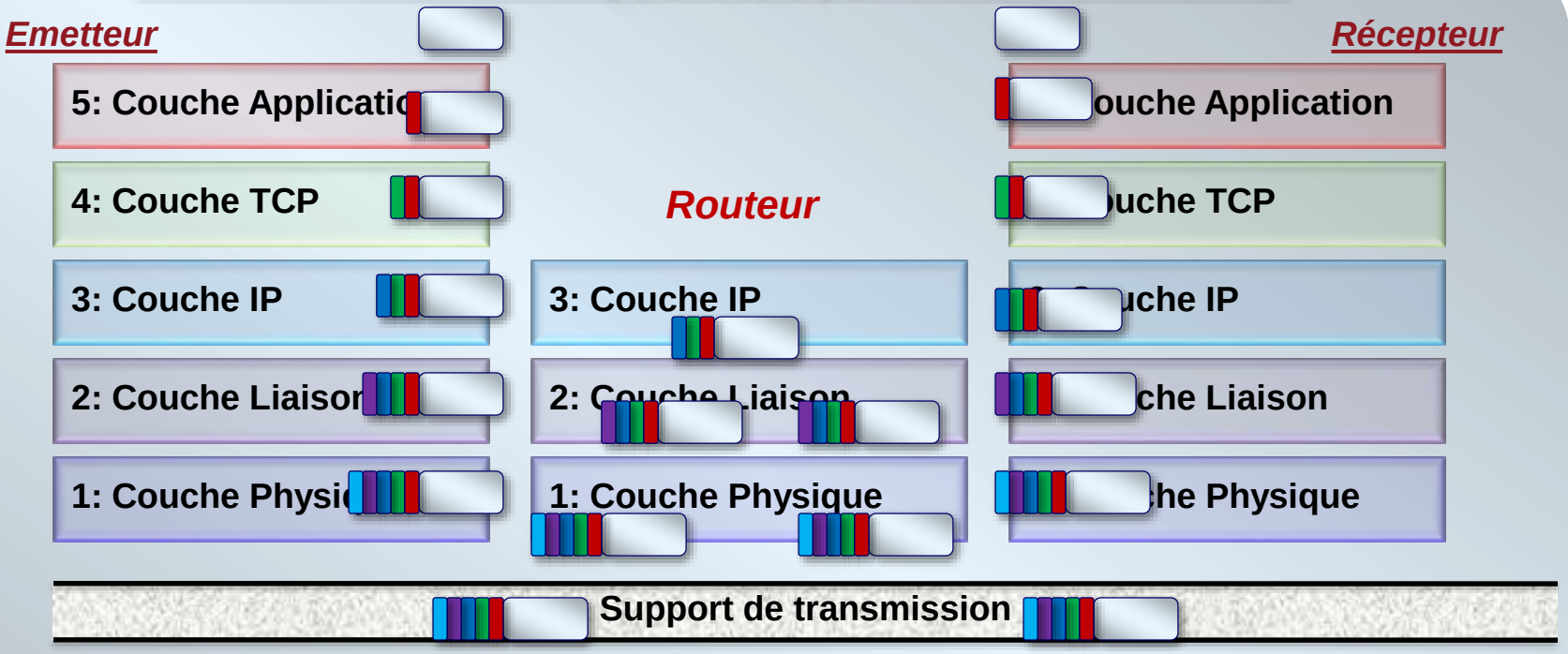
Pour pouvoir comprendre et gérer la sécurité informatique, il faut être conscients des différentes entités concernées.

Rappels

Nous aurons besoin des connaissances déjà acquises dans le domaine « Réseaux » ainsi que des « systèmes informatiques »

- **Les différentes couches réseau**

Rappels



- Couche N vers Couche N-1: ajout d'un champ d'informations : @source/@destination, contrôle d'erreur, taille paquet, N° ACK, …
- Protocole N: règle nécessaire au Service N
- Service de la Couche N: offert à la Couche N+1

Rappels

- Au niveau de chaque couche: plusieurs types d'attaques
- Au niveau de chaque couche: des mécanismes de sécurité pour contrer ces attaques.
- Connaissances robustes sur le fonctionnement des différentes couches pour bien comprendre le fonctionnement des attaques.
- Connaissances robustes sur les types d'attaques pour protéger le système informatique.
- Tout Système Informatique est menacé.
- Aucune solution de sécurité ne garantie à 100% protéger le système

Rappels

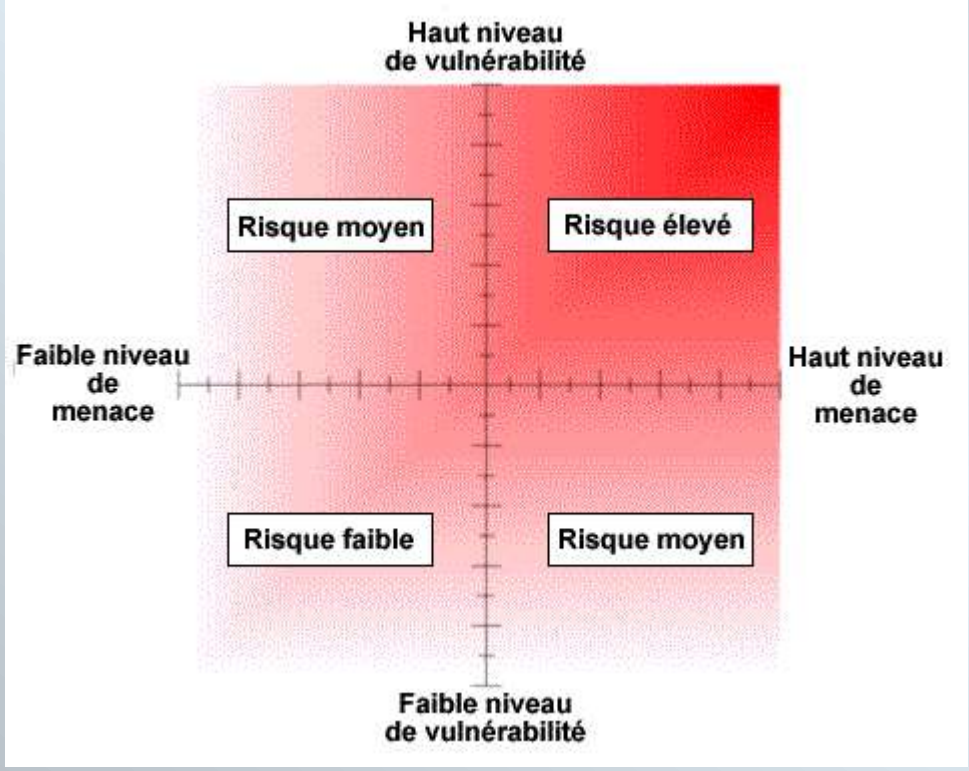
- Le système d'information est aujourd'hui un élément central du fonctionnement d'une organisation. Il peut être défini comme un ensemble de ressources (personnel, logiciels, processus, données, matériels, équipements informatiques et de télécommunication...) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations.

- Parmi les ressources informatiques figurent en particulier: les fichiers de données, bases de données et S.G.B.D, les outils de gestion des clients ou des collaborateurs, les outils de travail collaboratif, les serveurs d'application, les systèmes de workflow, les architectures d'intégration, les infrastructures réseaux.

Relation Risques, Vulnérabilités, Menaces (1)

Vulnérabilité + Menaces = Risques

- Loi qui régit plusieurs disciplines (pas que la sécurité informatique)



Relation Risques, Vulnérabilités, Menaces (2)

- **Menace**
  - ✓ Source Potentielle de danger qui peut causer un dommage au système ou des accès non-autorisés aux données.
- **Vulnérabilité**
  - ✓ Faille de sécurité qui rend un système vulnérable. Un système sans vulnérabilités est un système fiable. Il n'existe pas un système fiable à 100% sauf s'il est complètement isolé!
- **Attaque**
  - ✓ Action d'exploiter les failles pour avoir un accès illicite aux données ou empêcher le bon fonctionnement du système.

Objectifs de la Sécurité

- **Protéger contre tout usage illicite:**
  - ✓ Les machines (ordinateurs, serveurs, tablettes, smartphones, ….)
  - ✓ Les informations stockées
  - ✓ Les équipements réseau (routeurs, hub, …)
  - ✓ Les échanges de données sur le réseau

- **Assurer le bon fonctionnement du système**

en résumé, les objectifs sont:

- empêcher la divulgation non-autorisée de données
- empêcher la modification non-autorisée de données
- empêcher l'utilisation non-autorisée des ressources