Cours sécurité informatique

Mohamed Houcine HDHILI
med_elhdhili@yahoo.es

Karima MAALAOUI
karima.maalaoui@yahoo.fr

Objectifs du cours

- Acquérir des connaissances fondamentales sur les aspects de la sécurité des systèmes d'information
  - Services,
  - Attaques,
  - Mécanismes
- Apprendre comment choisir et déployer les mécanismes appropriées pour lutter contre les attaques.
- Acquérir des connaissances sur les méthodes cryptographique intervenant dans la plupart des mécanismes de sécurité

Plan du cours

- Enjeux de la sécurité informatique
- Vulnérabilités protocolaires et attaques réseaux
- Vulnérabilités logicielles et attaques Web
- Cryptographie
- Parefeux
- Système de détection et de prévention d'intrusions

Chapitre 1:
Enjeux de la sécurité informatique

Définition

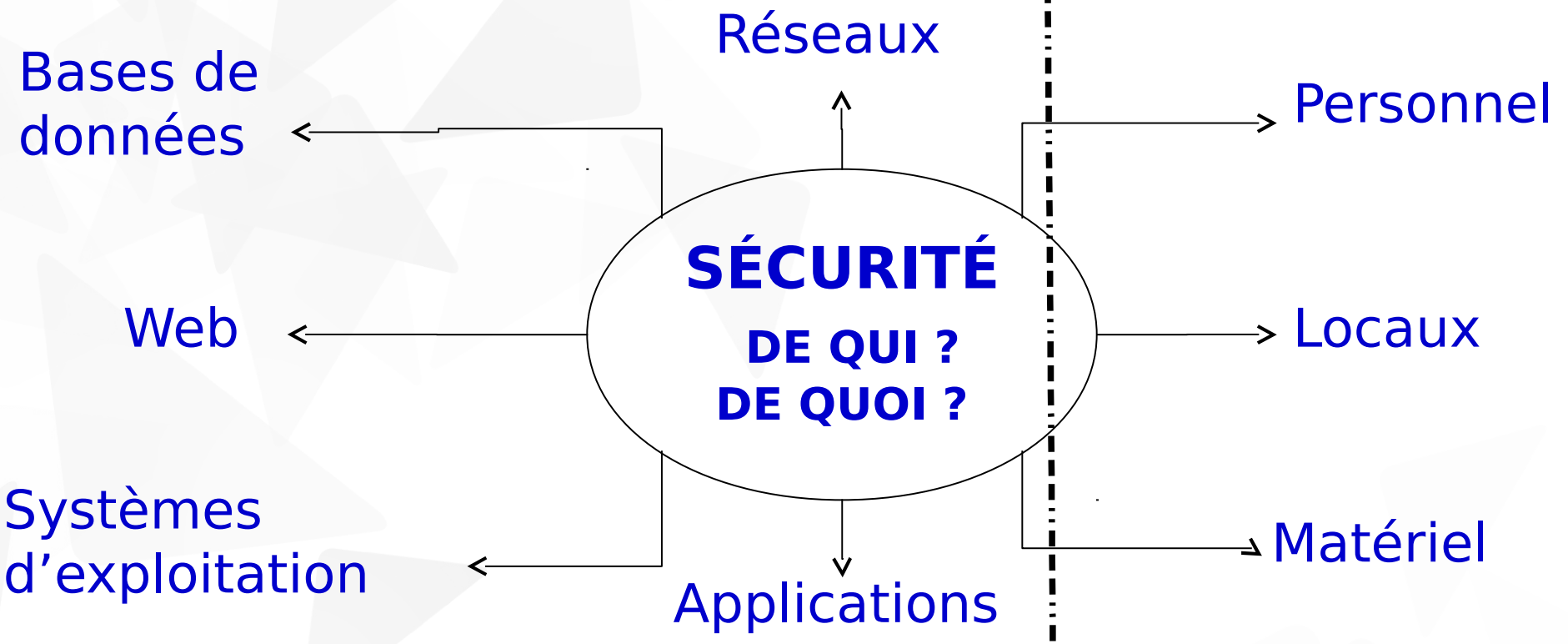
- Sécurité:
  - Ensemble des techniques qui assurent que les données et les ressources (matérielles ou logicielles) soient utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

    ➔Sécurité des systèmes d’informations

- Système d’information:
  - Ensemble d’activités consistant à gérer les informations: acquérir, stocker, transformer, diffuser, exploiter…
  - Fonctionne souvent grâce à un système informatique

➔ Sécurité du système d’information = sécurité du système informatique

Perimètre de la sécurité



1) Sécurité logique

Des données, des applications, des OS et des communications réseaux

2) Sécurité physique

- Contrôle d'accès physique
- Anti-incendie, dégâts d'eau
- Climatisation

3) Périmètre organisationnel:

répartition des responsabilités, sensibilisations des utilisateurs, contrôle, politique et guide de sécurité

Nécessité de la sécurité (1/2)

Avant.....ça ne nous intéresse pas

Ce n'est pas urgent

Je suis occupé

Ce n'est pas un problème

Les performances d'abord

Ça coute trop cher

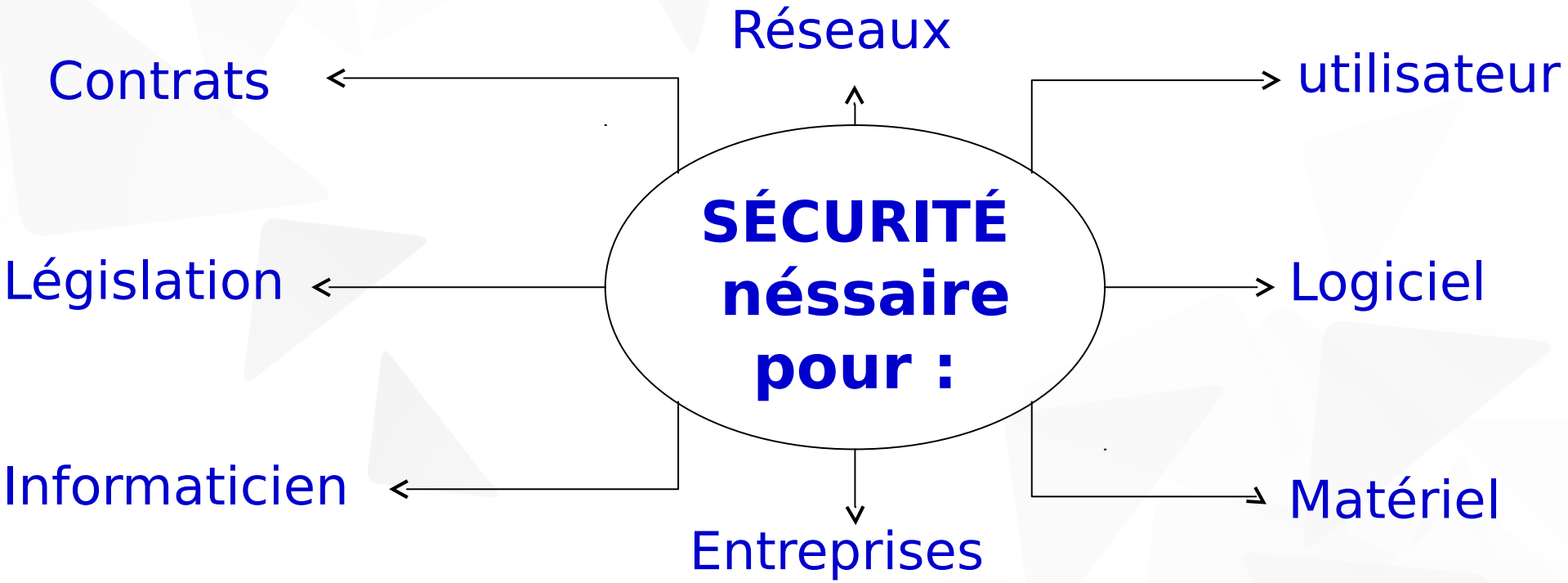
La communication d'abord

Mais, je n'ai rien à cacher.....

Nécessité de la sécurité (2/2)

Aujourd'hui.....

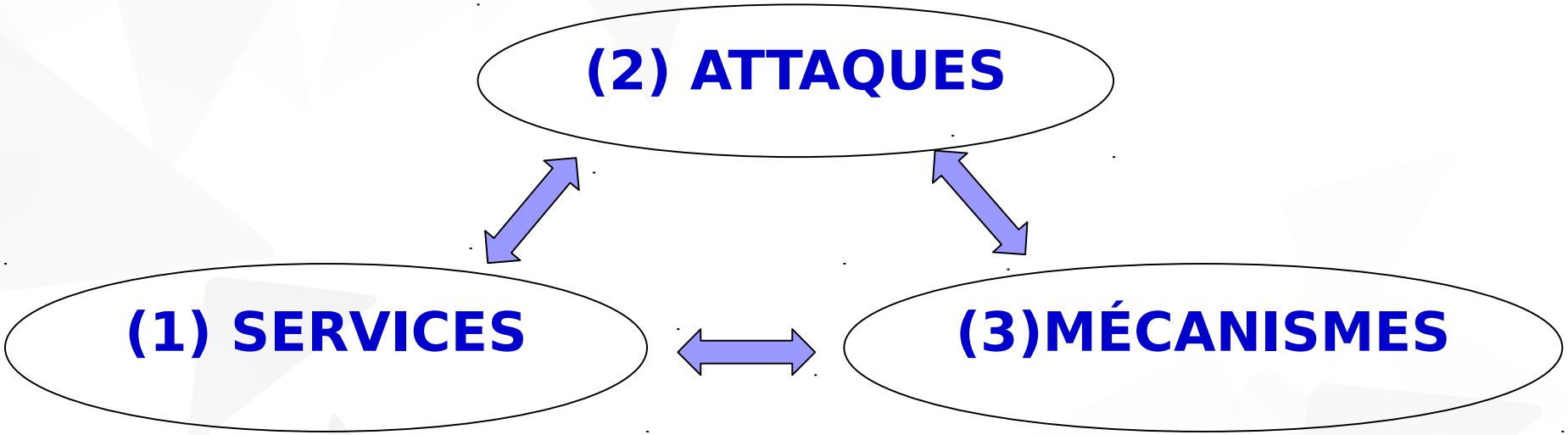
Besoin d'une stratégie de sécurité pour tous les domaines



-

Aspects de la sécurité

Actions exécutées pour casser les services de la sécurité en détournant les mécanismes



Fonctionnalités requises pour assurer un environnement sécurisé en faisant appel aux mécanismes

Moyens utilisés pour assurer les services de la sécurité en luttant contre les attaques

Aspects de la sécurité: services

Authentification

Assurance de l'identité d'un objet de tout type qui peut être une personne (identification), un serveur ou une application.

Intégrité

Garantie qu'un objet (document, fichier, message, etc.) ne soit pas modifié durant la communication.

Non répudiation

Assurance que l'émetteur d'un message ne puisse pas nier l'avoir envoyé et que son récepteur ne puisse pas nier l'avoir reçu.

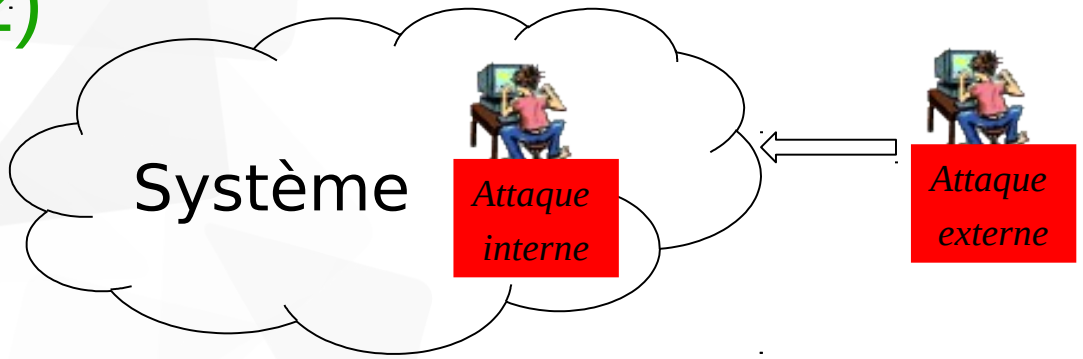
Confidentialité

Assurance qu'une information ne soit pas comprise par un tiers qui n'en a pas le droit

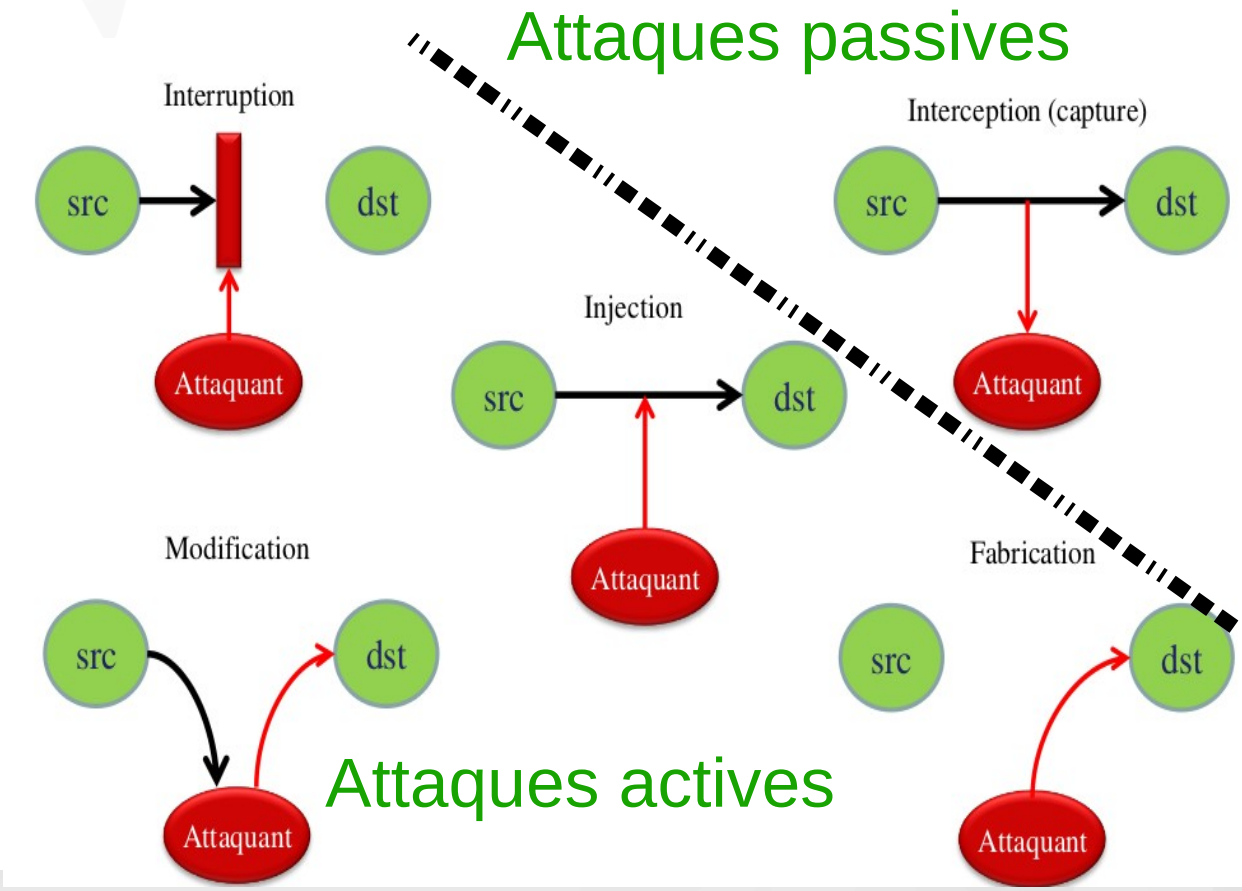
Disponibilité

Assurance que les services ou l'information soient utilisable et accessible par les utilisateurs autorisés

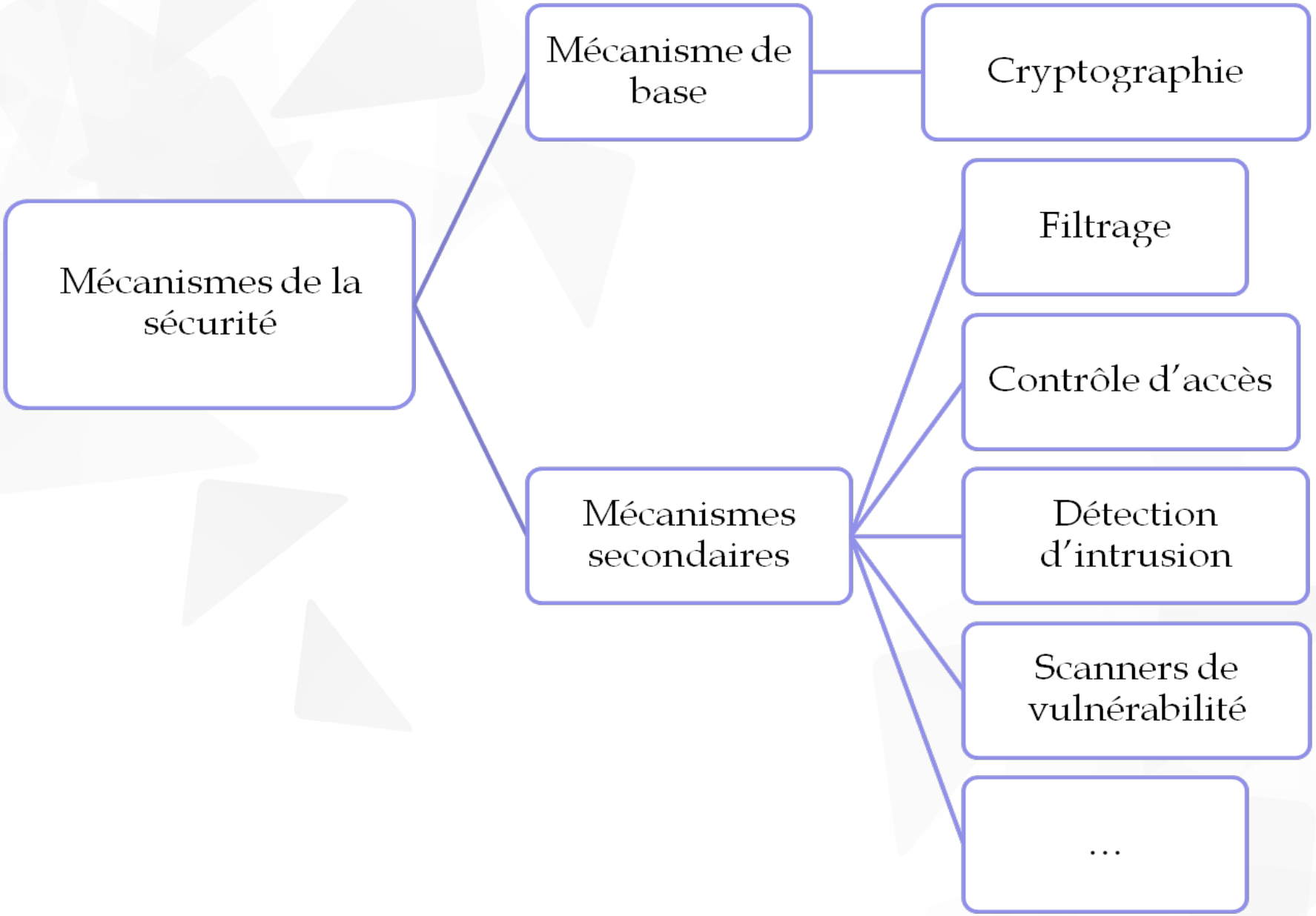
Attaques (1/2)



Type d'attaque	Propriétés visées
interception	confidentialité
interruption	disponibilité
injection	Integrité
modification	Confidentialité Integrité
fabrication	authenticité

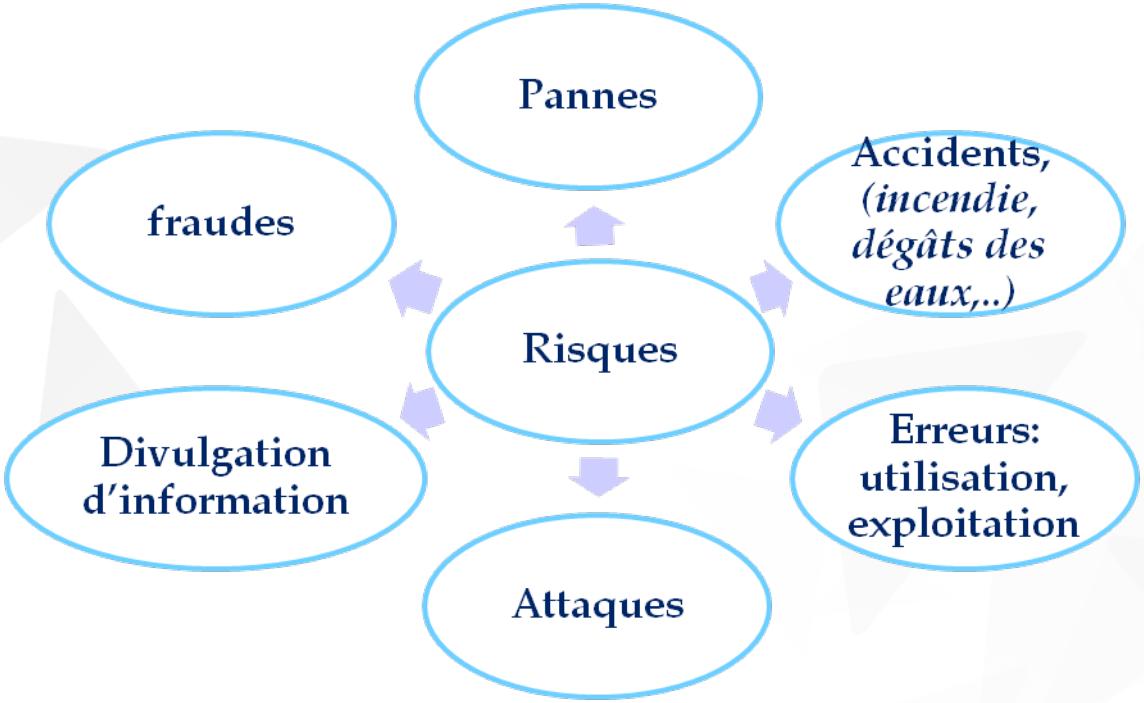


Aspects de la sécurité: mécanismes



Risque

- Le risque:
  - Le fait qu'un événement puisse empêcher de
    - Maintenir une situation donnée
    - Maintenir un objectif dans des conditions fixées
    - Satisfaire une finalité programmée



Politique de sécurité(1/2)

- Elaboration
  - **Après** l'analyse des risques
- Objectifs
  - Sécurisation adaptée aux besoins de l’entreprise
  - Compromis sécurité - fonctionnalité.
  - Permet d’analyser un audit de sécurité
- Composantes
  - politique de confidentialité
  - politique d’accès
  - politique d’authentification
  - Politique de responsabilité
  - Politique de maintenance
  - politique de rapport de violations
  - Etc.

Politique de sécurité(2/2)

- Etapes d’élaboration:
  - Identifier les risques et leurs conséquences.
  - Elaborer des règles et des procédures à mettre en œuvre pour les risques identifiés.
  - Surveillance et veille technologique sur les vulnérabilités découvertes.
  - Actions à entreprendre et personnes à contacter en cas de détection d'un problème.
- Etapes de mise en place:
  - Mise en œuvre
  - **Audit** et tests d'intrusion
  - Détection d'incidents
  - Réactions
  - Restauration

Audit sécurité

- Audit:
  - Mission d’examen et de vérification de la conformité (aux règles) d’une opération, d’une activité ou de la situation générale d’une entreprise

- Objectifs:
  - **Voir si la politique de sécurité est respectée**
  - Découvrir les risques
  - Effectuer des tests techniques de vulnérabilité
  - Proposer des recommandations
  - Proposer un plan d’action

A venir…

- … Attaques réseaux
- … vulnérabilités protocolaires