# Chapitre I : Introduction à la Sécurité Informatique

## I.1 Définitions

- **Sécurité (risque)** : Ensemble des mécanismes protégeant les systèmes d'information contre les actions malveillantes (ex. : attaques, vols de données).
- **Sûreté (panne)** : Assure la continuité et la fiabilité des systèmes contre les défaillances involontaires. Elle repose sur l'acronyme **RAMS** :
  - **Reliability (Fiabilité)** : Fonctionnement correct sur la durée.
  - **Availability (Disponibilité)** : Accès constant aux ressources.
  - **Maintainability (Maintenabilité)** : Facilité de réparation et de mise à jour.
  - **Safety (Sécurité)** : Protection contre les accidents.

**Lien OSI et sécurité** : Les attaques, mécanismes et services de sécurité s'intègrent dans le modèle OSI pour détecter, prévenir et répondre aux menaces.

### ➢ Concepts Clés

1. **Vulnérabilité** : Failles dans le système (ex. : bugs logiciels, mauvaise configuration) permettant des attaques.
2. **Menace** : Événement ou acteur potentiellement nuisible (ex. : hackers, logiciels malveillants).
3. **Risque** : Combinaison de la probabilité d'une menace et des impacts potentiels.
   - Modèle **DREAD** (Damage, Reproducibility, Exploitability, Affected users, Discoverability).
4. **Contre-mesures** : Mécanismes pour réduire ou éliminer les vulnérabilités et les menaces (ex. : pare-feu, audits).

### ➢ Objectifs de la Sécurité

- ➢ **Confidentialité** : Empêcher l'accès non autorisé aux données.
- ➢ **Intégrité** : Préserver l'exactitude et la cohérence des données.
- ➢ **Authentification** : Vérification de l'identité des utilisateurs.
- ➢ **Disponibilité** : Garantir l'accès aux ressources lorsqu'elles sont nécessaires.
- ➢ **Non-répudiation** : Preuve irréfutable des actions réalisées par un utilisateur.

# II Menaces et risque

Les concepts **STRIDE** et **DREAD**, développés par Microsoft, permettent respectivement de **classer les types de menaces** et de **mesurer les risques associés**.

## 1- STRIDE : Classification des menaces

Le modèle **STRIDE** identifie **six types principaux de menaces** qui peuvent affecter un système informatique. Chaque type est lié à un **objectif de sécurité** particulier.

| Type de menace | Description | Impact sur la sécurité | Exemple |
|---|---|---|---|
| **S : Spoofing** | Usurpation d'identité. Une entité malveillante se fait passer pour une autre. | Compromet l'identification | Un pirate se fait passer pour un utilisateur légitime en volant ses identifiants (phishing). |
| **T : Tampering** | Modification non autorisée de données ou de code. | Compromet l'intégrité | Un attaquant modifie un fichier de configuration pour donner un accès administrateur. |
| **R : Repudiation** | Négation d'une action réalisée par un utilisateur. | Compromet la non-répudiation | Un utilisateur prétend ne pas avoir envoyé une commande d'achat, faute de preuve d'authenticité. |
| **I : Information Disclosure** | Divulgation non autorisée d'informations sensibles. | Compromet la confidentialité | Une fuite de mots de passe via une faille de configuration d'un serveur Web. |
| **D : Denial of Service (DoS)** | Blocage d'un service légitime en surchargeant les ressources du système. | Compromet la disponibilité | Une attaque DoS paralyse un site Web en l'inondant de requêtes. |
| **E : Elevation of Privilege** | Un utilisateur obtient des privilèges qu'il n'est pas censé avoir. | Compromet l'autorisation | Un utilisateur standard exploite une faille pour devenir administrateur d'un système. |

- **STRIDE** décrit **ce qui peut arriver** (les types de menaces).

## Exemple combiné :

Lors d'une attaque sur un site Web :

1. **Spoofing** : Le pirate usurpe l'identité d'un utilisateur avec des identifiants volés.
2. **Tampering** : Il modifie les transactions pour détourner des fonds.
3. **Repudiation** : Il tente de nier avoir effectué ces transactions.
4. **Information Disclosure** : Il vole des informations sensibles des utilisateurs.
5. **Denial of Service** : Il surcharge le serveur pour bloquer l'accès des utilisateurs légitimes.
6. **Elevation of Privilege** : Il exploite une faille pour prendre le contrôle total du site.

## 2- DREAD : Évaluation des risques

Le modèle **DREAD** aide à **quantifier le niveau de risque** d'une menace en évaluant plusieurs facteurs. Chaque facteur est noté sur une échelle (par exemple, de 1 à 3), et le score total permet de prioriser les menaces.

| Facteur | Description | Question à se poser | Exemple |
|---|---|---|---|
| **D : Damage** | Dommages potentiels causés par la menace. | Quelle est la gravité des dommages si la menace se réalise ? | Vol de données sensibles comme des numéros de carte de crédit. |
| **R : Reproducibility** | Facilité avec laquelle la menace peut être reproduite. | L'attaque peut-elle être facilement répétée ? | Une attaque de phishing peut être reproduite avec un email malveillant. |
| **E : Exploitability** | Difficulté pour exploiter la menace. | Quelle est la facilité pour lancer l'attaque ? | Une vulnérabilité connue avec des outils publics rend l'exploitation facile. |
| **A : Affected Users** | Nombre d'utilisateurs potentiellement affectés. | Combien d'utilisateurs sont concernés ? | Une faille dans une application bancaire en ligne affecterait des milliers d'utilisateurs. |
| **D : Discoverability** | Facilité avec laquelle la vulnérabilité peut être découverte. | L'attaque est-elle visible ou difficile à détecter ? | Une mauvaise configuration d'un pare-feu peut être détectée par un simple scan réseau. |

- **DREAD** quantifie **l'impact des menaces identifiées** (priorisation des risques).

## Formule :

Niveau de risque = Damage+Reproducibility+Exploitability+Affected Users+Discoverability\text{Damage} + \text{Reproducibility} + \text{Exploitability} + \text{Affected Users} + \text{Discoverability}

- **Risque élevé** : Score total de 12 à 15.
- **Risque moyen** : Score total de 8 à 11.
- **Risque faible** : Score total de 0 à 7.

**Exemple avec DREAD :**

Supposons une faille X dans une application de paiement :

- **Damage (3)** : Si exploitée, elle permet de voler les fonds des utilisateurs.
- **Reproducibility (3)** : Une fois connue, elle est facilement exploitable.
- **Exploitability (2)** : L'exploitation nécessite des connaissances techniques modérées.
- **Affected Users (3)** : Tous les utilisateurs de l'application sont concernés.
- **Discoverability (2)** : La faille est visible pour ceux qui analysent les requêtes réseau.

**Score total** : 3+3+2+3+2=133 + 3 + 2 + 3 + 2 = 13. **Risque élevé**.