Sécurité informatique

Risques et Enjeux

Plan

1. **Introduction**
2. **Un mot sur le TP**
3. **Cryptographie**

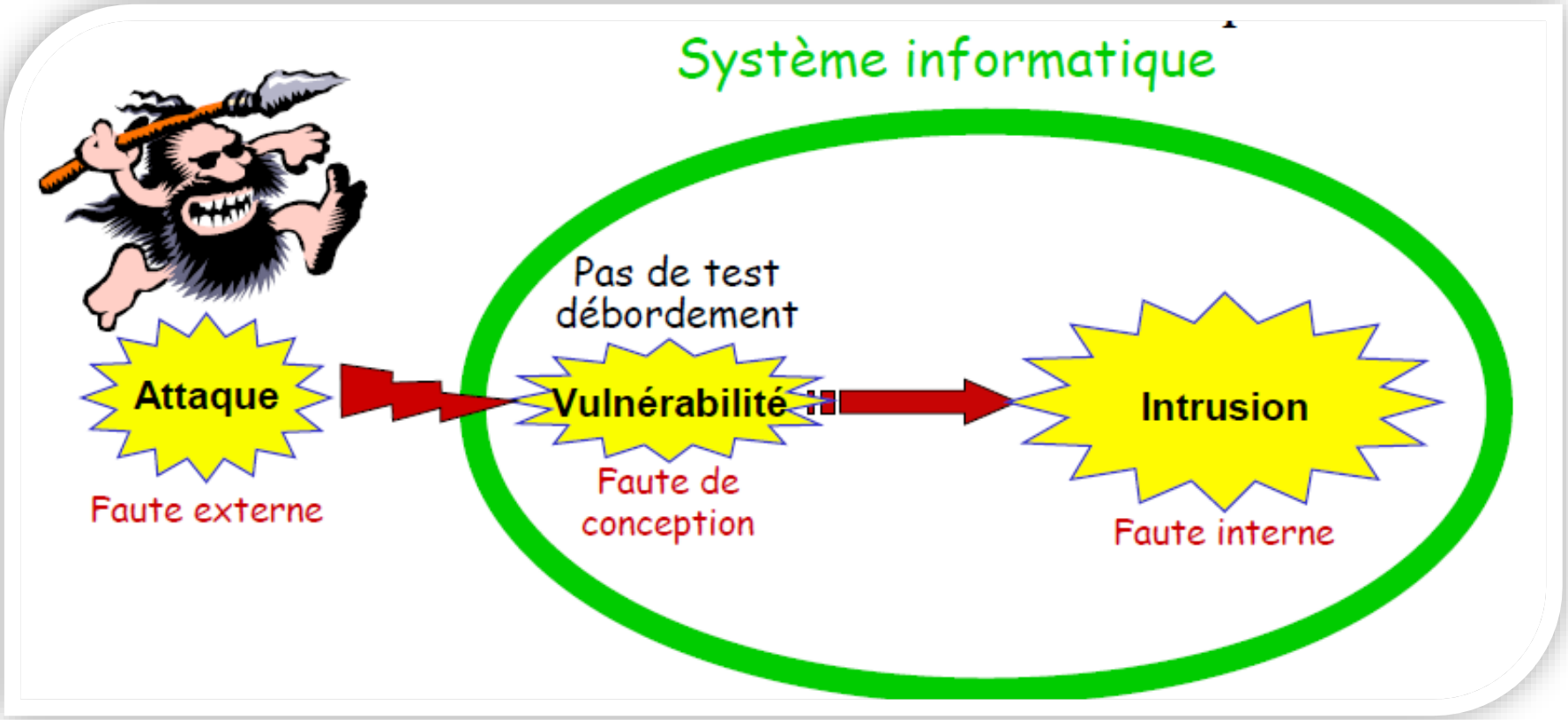
Plan

1. **Introduction**
2. Un mot sur le TP
3. Cryptographie

Introduction

- Une **menace** est un événement ou une opération malveillante ou pas, qui pourrait nuire à une ressource.
- Une **vulnérabilité** est une faiblesse qui rend possible une menace
  - peut être due à une mauvaise conception,
  - à des erreurs de configuration ou
  - à des techniques de codage inappropriées et non fiables
- Une **attaque** est une action qui exploite une vulnérabilité ou exécute une menace. Par ex., envoyer des données d'entrée malveillantes à une application ou saturer un réseau en vue d'entraîner un refus de service.

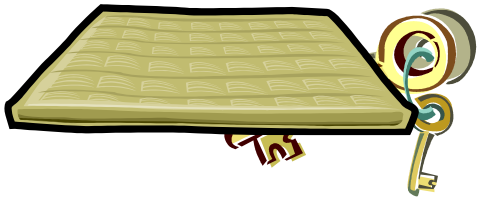
Introduction



Introduction

Un risque ne peut être éliminé. Il peut seulement être réduit soit par la mise en place de meilleures protections soit en réduisant l'impact.

$$\text{Risque} = \frac{\text{Vulnérabilité} \bullet \text{Menace} \bullet \text{Impact}}{\text{Contre mesure}}$$



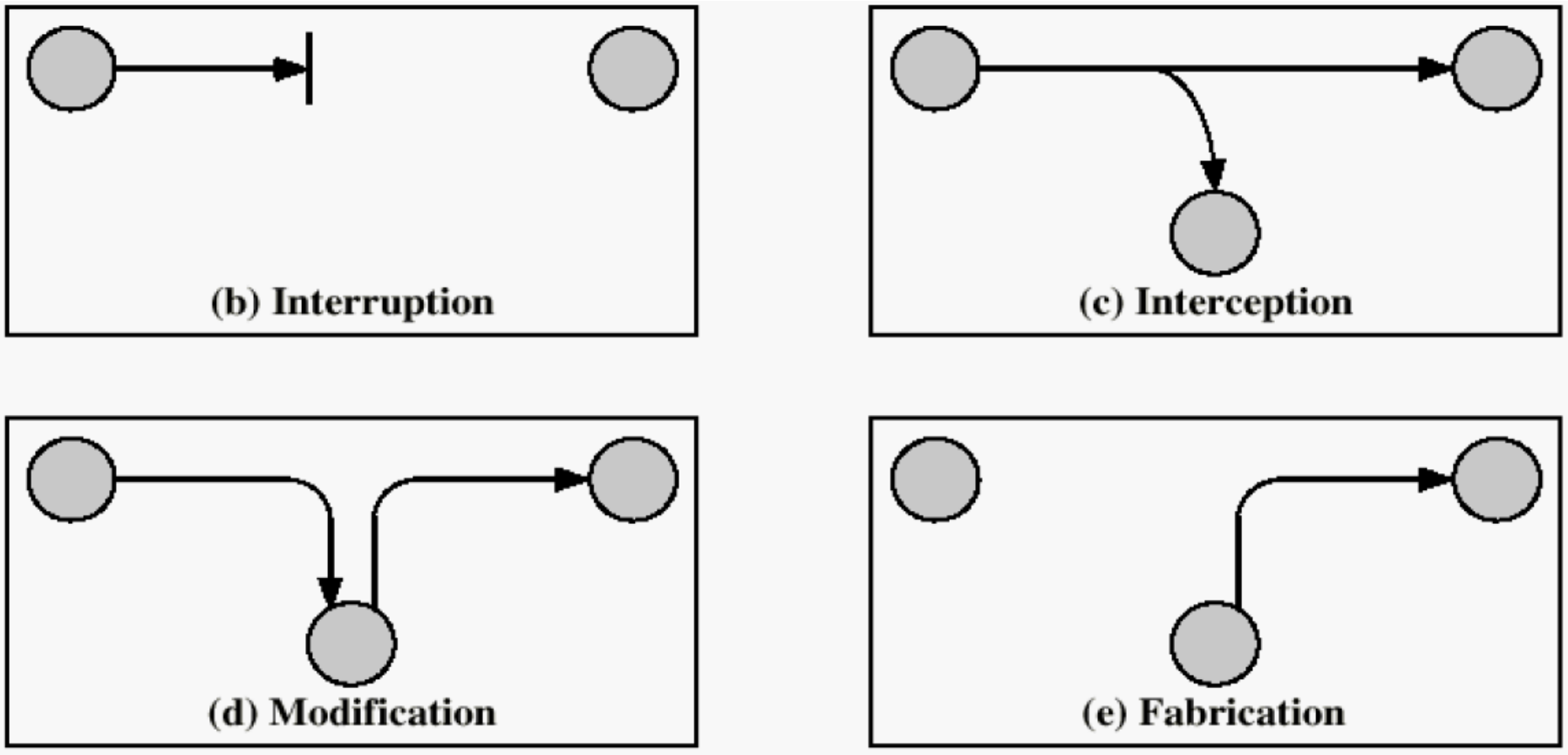
Vulnérabilité:
Clés sous le tapis.

Menace:
Cambrioleur essaie d'entrer.

Impact: Cambrioleur casse l'armoire, vole de l'argent, crée des ennuis.

Introduction

Sécurité = c'est l'ensemble des mesures permettant d'assurer la protection de l'information & des Systèmes



Pourquoi Attaquer ?

- **Gain financier:** Récupération des num. de cartes bancaires, ...
- **Vengeance:** Site www.aljazeera.net lors de la couverture de la guerre d'irak
- **Curiosité:** Attaques d'étudiants du MIT sur le premier ordinateur IBM 704 au MIT en 1959.
- Recherche d'émotions fortes

Plan

1. Introduction
2. **Un mot sur le TP**
3. Cryptographie

Un mot sur le TP

Description

- En sortant de l'ordinaire, le TP du module de « Sécurité des systèmes informatiques» se déroulera sous forme d'exposés faits par les étudiants de Master 2.
- Les exposés portent sur la thématique pure de la sécurité des systèmes, y compris les réseaux et les bases de données.
- Le rapport doit être rédigé en **Latex**, et la présentation en **Beamer**.

Un mot sur le TP

Objectifs du TP:

Étaler et comprendre les menaces et attaques visant les systèmes, et mettre en place des mécanismes de protection ou d'éradication si possible, donc pour résumé, l'objectif est le suivant :

1. **Comment détecter l'attaque ou le programme malveillant ?**
2. **Comment mettre fin à cette attaque ou ce programme malveillant ?**
3. **Comment se protéger de cette attaque ou de ce programme malveillant ?**

Un mot sur le TP

Thèmes du TP:

Programmes Malveillants:

1. Virus
2. Vers (Worm)
3. Spyware (keylogger)
4. Bombe Logique
5. Porte dérobée
6. Cheval de Troie

Un mot sur le TP

Attaques Malveillantes:

1. Usurpation d'adresse IP (Spoofing IP)
2. Déni de service (Smurf, ping de la mort, Synflood)
3. ARP Poisoning & DNS Poisoning
4. Phishing & hoax
5. Injection SQL
6. XSS : Cross-Site Scripting
7. Stack overflow

Un mot sur le TP

Présentation:

Chaque binôme ou monôme présentera son exposé lors de la séance de TP. La présentation se compose:

- d'une partie **théorique** ne devant pas dépasser les 20 minutes,
- et d'une partie **pratique** de 20 minutes au maximum, qui dépendra du sujet en question et qui peut être soit une simulation par un logiciel ou une vidéo, soit une implémentation réalisée par l'étudiant lui-même, **c'est le cas idéal**.

Un mot sur le TP

Après-présentation

Après avoir terminé la présentation, on ouvre un débat sur le sujet via des questions posées par les étudiants et l'enseignant chargé du TP.

Évaluation

- La note de l'exposé fera l'objet de la note du **CC3**, qui varie entre **0** (*celui qui n'a rien fait ou s'est absenté*) et **16**/20.
- Toute absence **justifiée** de l'étudiant intéressé entraine automatiquement une note de 8/20 au CC3

Plan

1. Introduction
2. Un mot sur le TP
3. **Cryptographie**

Cryptographie

- **Algorithmes de chiffrement faibles**

  Chiffre de César, Chiffre de Vigenère.

- **Algorithmes de cryptographie symétrique**

  Chiffre de Vernam, DES, 3DES, AES, RC4, RC5

- **Algorithmes de cryptographie asymétrique**

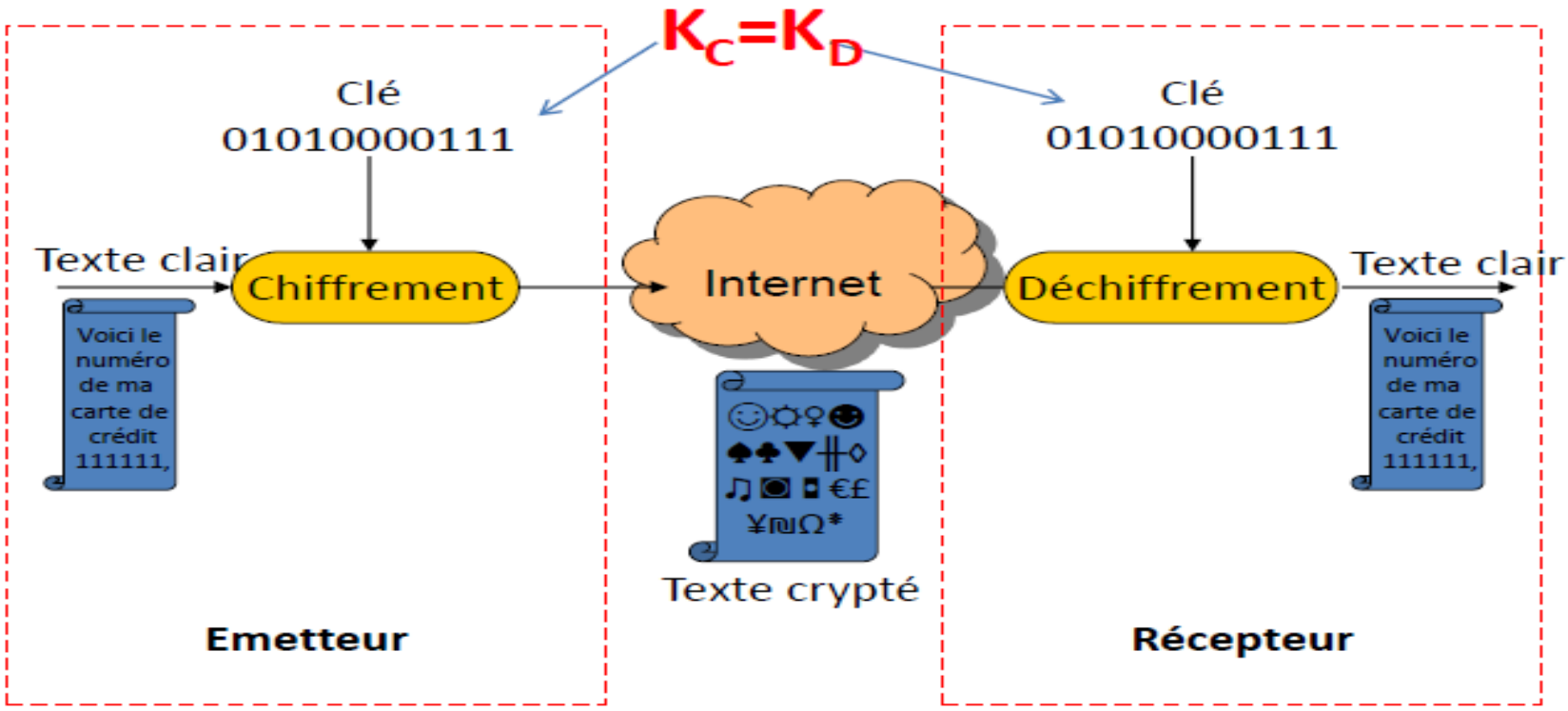
  RSA (chiffrement et signature), DSA (signature) Diffie-Hellman (échange de clé)

- **Fonctions de hachage**

  MD5, SHA-1, SHA-256 ;

Chiffrement Symétrique

Dans la plupart des cryptosystèmes symétriques (appelés aussi systèmes de chiffrement à **clé privée**), la clé de chiffrement est la **même** que la clé de déchiffrement.



Chiffrement Symétrique

Ainsi on définie:

- L'ensemble **K** de toutes les clés possibles $\mathbf{K=\{0,1\}^L}$
- L'ensemble **M** de tous les messages en claires $\mathbf{M=\{0,1\}^*}$
- L'ensemble **C** de tous les messages chiffrées $\mathbf{C=\{0,1\}^*}$

Chiffrement Symétrique

Un algorithme de chiffrement symétrique est définie par deux fonctions **E** et **D** (un couple (E,D)), tel que:

$$\mathbf{E}: K \times M \rightarrow C$$

$$(k,m) \rightarrow c = E(k,m) = E_k(m)$$

et

$$\mathbf{D}: K \times C \rightarrow M$$

$$(k,c) \rightarrow m = D(k,c) = D_k(c)$$

et aussi:

$$\forall\ \mathbf{m} \in \mathbf{M}, \forall\ \mathbf{k} \in \mathbf{K}: \mathbf{D}(\mathbf{k}, \mathbf{E}(\mathbf{k}, \mathbf{m})) = \mathbf{m}$$

E: peut être aléatoire , mais **D** doit être déterministe.

Chiffrement Symétrique

Deux catégories existent pour le chiffrement symétrique:

1. **Chiffrement par flot (Stream Cipher):**

   Les données en claires sont considérées comme un **flot** de **bits** (**octets**) et sont chiffrées ensembles.

2. **Chiffrement par bloc (Block Cipher):**

   Les données en claires sont considérées **bloc** par **bloc** (de taille fixe). Les blocs sont ensuite chiffrés selon un mode opératoire spécifique. (généralement, il est plus sécurisé que le chiffrement par flot !)

Le plan à suivre

1. **Chiffrement par Flot**
2. **Chiffrement par Bloc**
3. **Modes opératoires**
4. **Intégrité des messages**
5. **Fonctions de hachage**
6. **Chiffrement authentifié**
7. **Échange et établissement de clés**
8. **RSA & ElGamal** *(Si on aura le temps)*