Chapitre I :

Enjeu de la sécurité informatique

Plan

1.1 Définition de la sécurité informatique

1.2 Objectifs de la sécurité informatique

1.3 Les différentes catégories d’attaques et leurs risques

Définition de la sécurité informatique

La sécurité informatique représente des :

- Moyens organisationnels : Règles [1]

- Moyens Techniques [1]
  - Ressources matérielles (Firewalls, proxy…)
  - Ressources logicielles (Antivirus, Antispam…)

Qui sont mis en place pour protéger notre système d'information(1).

Enjeu de la sécurité informatique

1.1 Définition de la sécurité informatique

1.2 Objectifs de la sécurité informatique

1.3 Les différents types d’attaques et leurs risques

Objectifs de la sécurité informatique

La sécurité informatique doit garantir :

- Le fonctionnement optimal de l'ensemble de machines.
- L'attribution des droits spécifiques à des utilisateurs bien déterminé

Objectifs de la sécurité informatique

En outre, doit être capable de :

- Empêcher des personnes non autorisés d'accéder au système.

- Empêcher des utilisateurs d'effectuer des opérations involontaires/volontaires capables de nuire au système.

- Sécurisé les données

- Garantir la non interruption d'un service

Objectifs de la sécurité informatique

La sécurité informatique vise à assurer [2] :

- **L'intégrité** : Les données ne sont modifié que par des personnes ayant le droit.
- **La confidentialité** : les données échangés entre deux correspondant ne peuvent pas être consulté par un tiers.
- **L'authentification** : les personnes utilisant une ressource correspondent aux noms d'utilisateurs.
- **La disponibilité** : les données ainsi que les ressources matérielles sont accessibles lors du besoin
- **La non-répudiation** : aucun correspondant ne peut nier la transaction qu'il a réalisé.

Les différentes catégories d’attaques et leurs risques

- Les différentes catégories d’attaques
- Les risques des attaques

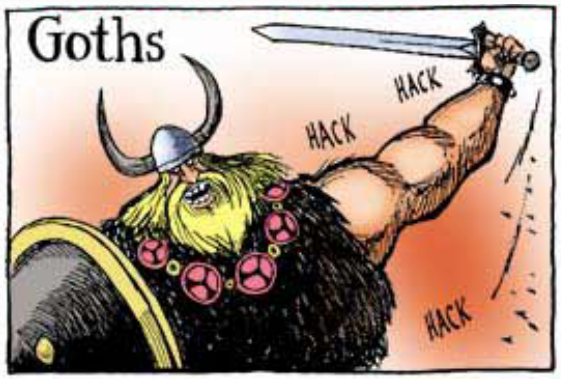
Les différentes catégories d'attaques

- Une attaque représente un ensemble de techniques/moyens visant à nuire à un système d'information.

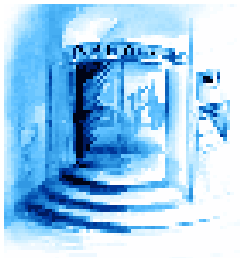
- Elle peut être :

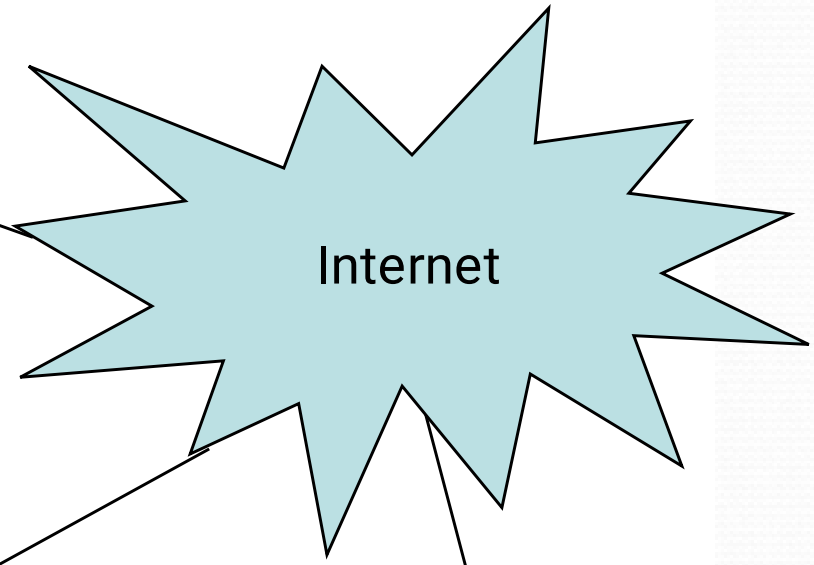
  - Active ou passive

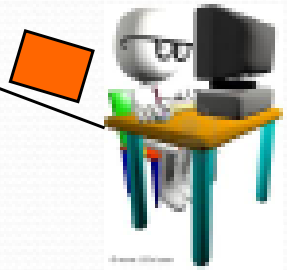
  - Directe ou indirecte

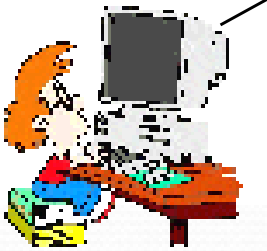


Attaques Passives [1]









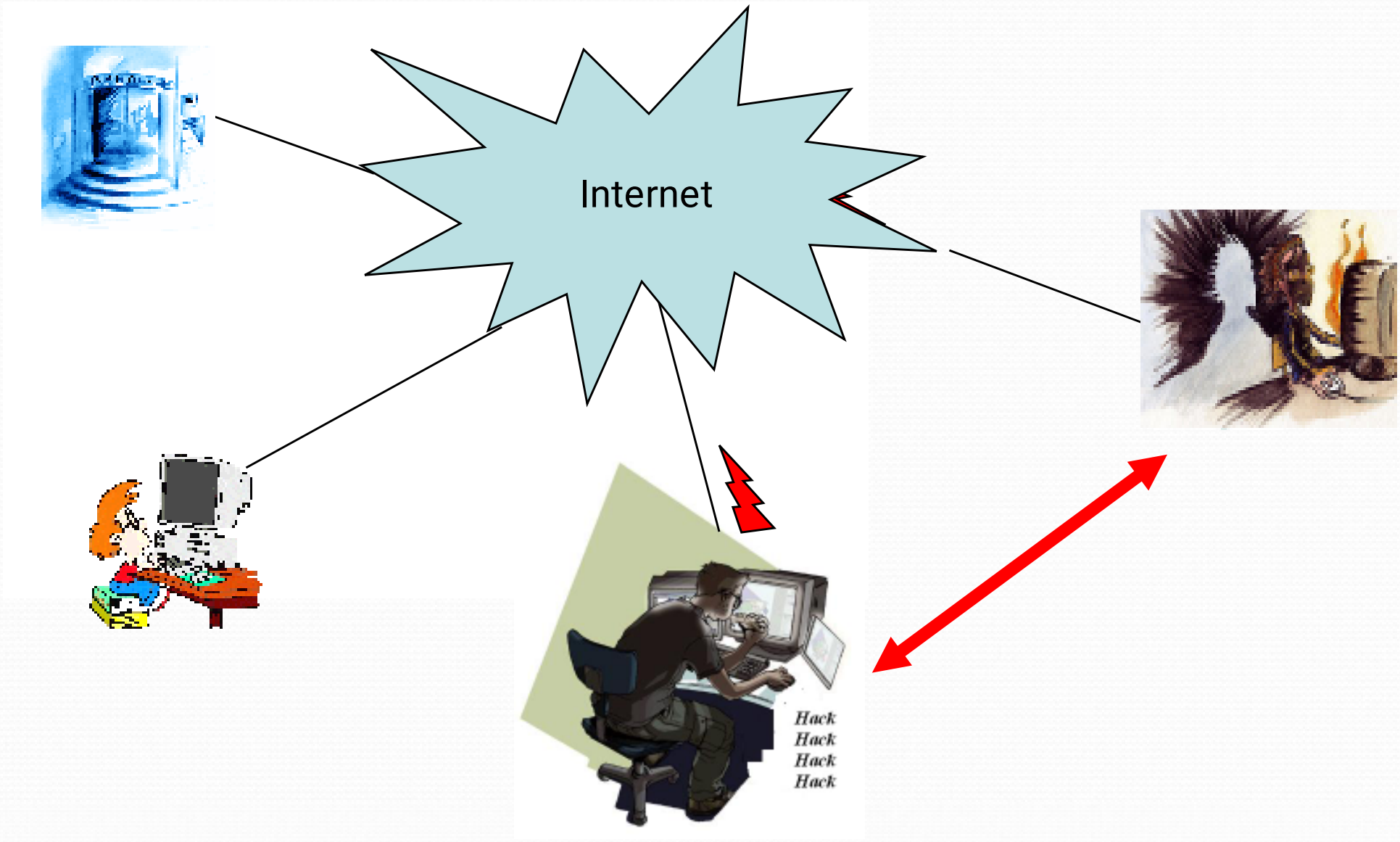
- Analyser le flux de données
- Récupération des login/mots de passe…
- …

Attaques actives

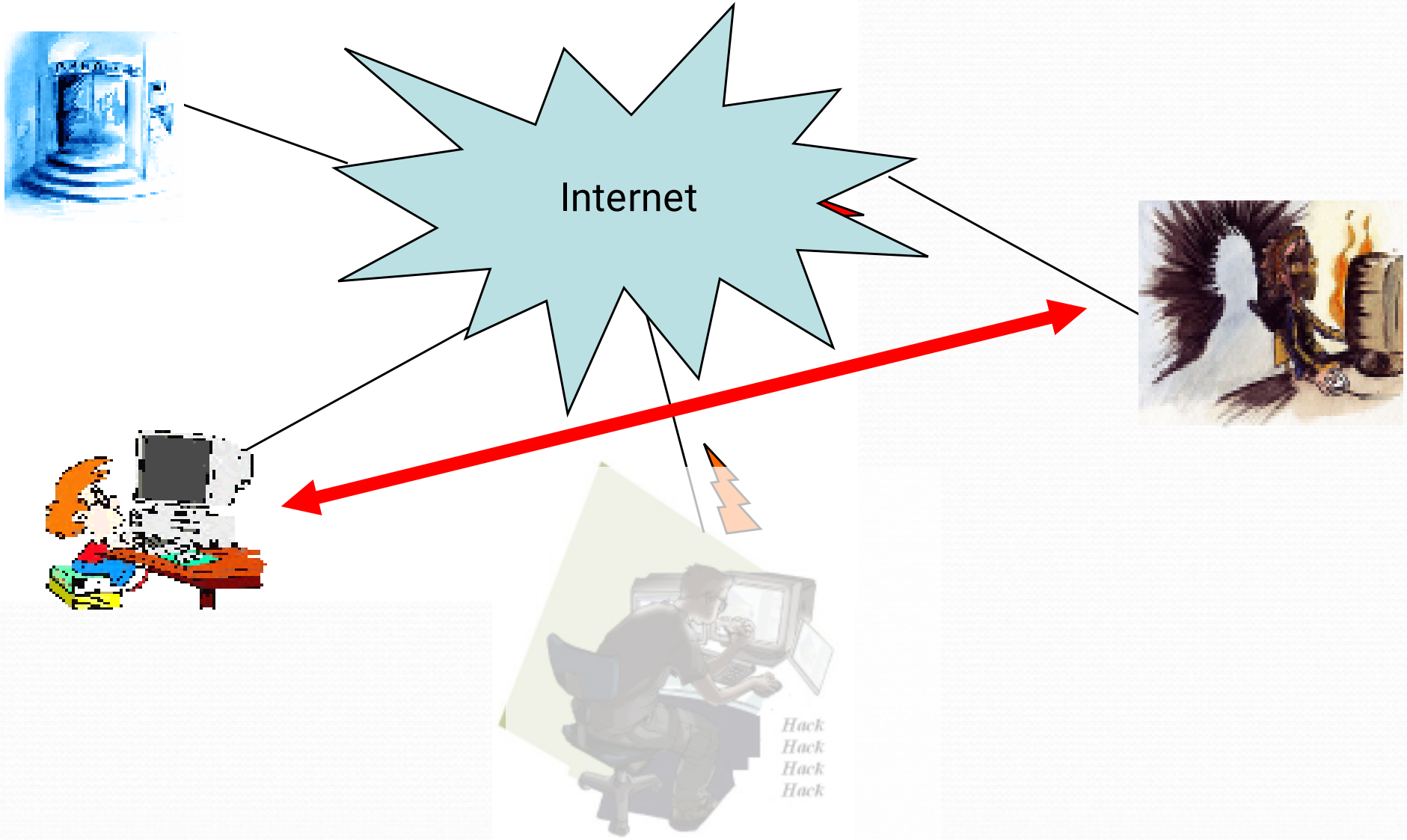
Internet

- Envoi de commandes
- Utilisation des chevaux de Troie, des vers…
- Dépassement de tampon
- Déni de service

Attaques directes



Attaques indirectes (par rebondissement)



Les risques des attaques

- Atteinte à la disponibilité
- Atteinte à la confidentialité
- Atteinte à l'intégrité
- Atteinte à l'authenticité

Les risques des attaques: Atteinte à la disponibilité

- Le système devient indisponible ou inutilisable.

➔ Interruption du fonctionnement du système

Exemple :

- Destruction matérielle : d'un support de stockage (disque Dur), d'un équipement d'interconnexion (hub, switch, modem, routeur..), coupure d'une ligne de communication…

- Destruction logicielle d'une machine en causant un disfonctionnement du système d'exploitation…

Les risques des attaques

- Atteinte à la disponibilité
- Atteinte à la confidentialité
- Atteinte à l'intégrité
- Atteinte à l'authenticité

Les risques des attaques: Atteinte à la confidentialité

L'attaquant obtient un accès à des ressource/des données d'une manière illégitime

➔ Interception des données

Exemple

- Vol de mots de passe/login
- Accès à des serveurs…

Les risques des attaques

- Atteinte à la disponibilité
- Atteinte à la confidentialité
- Atteinte à l'intégrité
- Atteinte à l'authenticité

Les risques des attaques: Atteinte à l'intégrité

L'attaquant accède au contenu d'une ressource et le modifie de façon indétectable.

➔ modification du contenu

Exemple :

- Suppression d'un fichier au niveau d'un serveur
- Supprimer du contenu d'un ficher
- Modification du contenu des messages échangés

Les risques des attaques

- Atteinte à la disponibilité
- Atteinte à la confidentialité
- Atteinte à l'intégrité
- Atteinte à l'authenticité

Les risques des attaques: Atteinte à l'authenticité

L'attaquant insère de fausses informations/données dans le système cible.

➔ Fabrication de messages/d'information

Exemple

- Injection de faux messages dans le réseau

Glossaire

(1) Système d’information : est composé par des composantes (matérielles, logiciels, personnels, et données) dans une organisation.

Références

[1] Document de formation de l'Agence National de Sécurité Informatique, 2005, en partie disponible dans http://www.ansi.tn/fr/documentations/publications.html

[2] Patrick Ducrot, "Sécurité informatique", cours de sécurité à L'Ecole Nationale Supérieur des ingénieurs Caen, 2012.