Cours : Cryptographie et Sécurité Informatique

Objectifs du cours :
(1) Offrir une première vision de la sécurité informatique.

(2) Sensibiliser les étudiants à la sécurité des systèmes informatiques.

(3) Développer des compétences pratiques liées à la sécurité informatique.

(4) Découvrir différentes méthodes cryptographique de chiffrement de données.

(5) Coder ces méthodes dans un langage de programmation.

Cours : Cryptographie et Sécurité Informatique

Chapitre 1
Introduction à la Sécurité Informatique

I. Akharraz
Université Sidi Mohamed Ben Abdellah

ismail.akharraz@usmba.ac.ma

Sommaire

1. Pourquoi la sécurité informatique?.
2. Définitions et concepts de base.
3. Objectifs de la sécurité informatique.
4. Vulnérabilité.
5. Les menaces.
6. Les attaquants.
7. Les outils de défenses.
8. La cryptographie.

1. Introduction : pourquoi la sécurité informatique?.

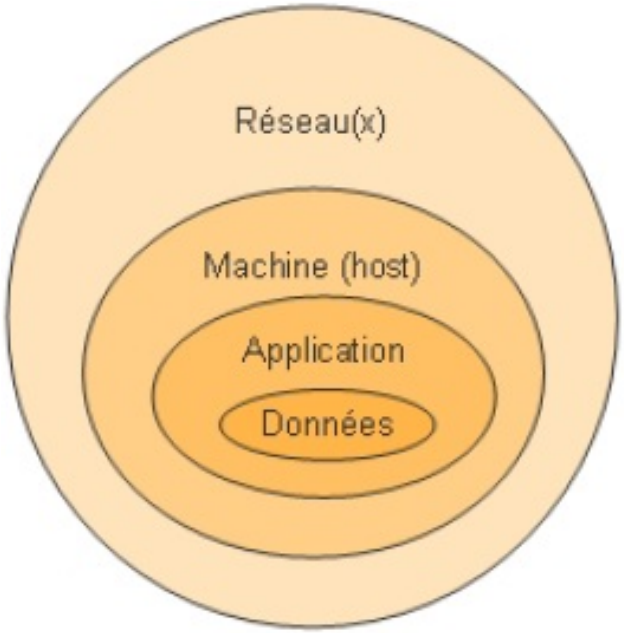
- Les systèmes d'informations se basent sur des systèmes informatiques de plus en plus complexes pour la diffusion de l'information.

- Un système informatique est exposé à :
  - Refuser de faire quoi que ce soit (plantage).
  - Faire des actions différentes de celles attendues.
  - Etre attaqué par un pirate avec pour conséquence:
    - La destruction de données.
    - La transformation de votre écran en une oeuvre d'art minimaliste.
    - L'inondation de la planète de messages insultants.

1. Introduction : pourquoi la sécurité informatique?

- L'espionnage de votre comportement et la vente de ces informations.
- L'utilisation de votre machine comme relai d'attaque.
- L'implantation d'un module de surveillance.

- Tout système d'informations est vulnérable : besoin de protection des informations digitales.
- La sécurité doit être présente à plusieurs niveaux:



2. Définitions et concepts de base.

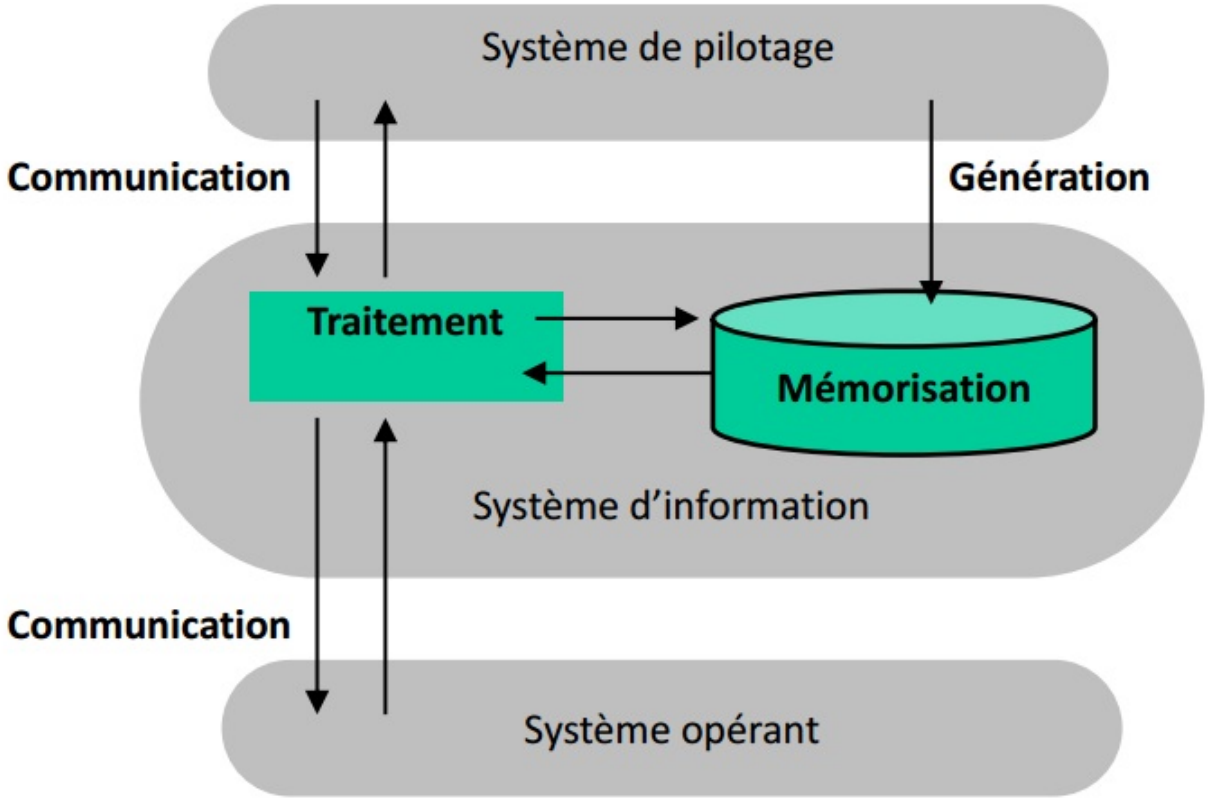
Définition

Un Système d'information (SI) est l'ensemble des moyens nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des informations.

Un SI comprend :

- Les données.
- La manière d'organiser et de structurer les données.
- Les moyens mis pour le traitement des données.
- Les moyens mis pour élaborer, véhiculer et rendre disponible l'information.

- Représentation systémique d'une organisation :



2. Définitions et concepts de base.

On remarque que :

- Le SI représente un patrimoine précieux de l'organisation.

- La confidentialité et la disponibilité de l'information constitue un enjeu très important pour la compétitivité de l'entreprise.

- Protéger ce patrimoine est donc crucial pour une entreprise.

Définition

La sécurité du système d'information est l'ensemble de mesures de sécurité physique, logique, administrative et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer:

- *La confidentialité des données du SI.*
- *L'intégrité des données du SI.*
- *La disponibilité de ces données (continuité du service).*

- `La sécurité informatique concerne la partie automatisée du SI : Système Informatique.`

2. Définitions et concepts de base.

- La sécurité d'un système informatique a pour mission principale la protection des informations et des ressources contre toute divulgation, altération ou destruction.

- L'accès à ces ressources doit être également protégé et un accès autorisé à ces ressources ne doit pas être refusé.

- La sécurité informatique consiste à utiliser tous les mécanismes disponibles pour garantir les propriétés suivantes : la confidentialité, l'intégrité et la disponibilité.

2. Définitions et concepts de base.

- Les systèmes informatiques sont au coeur des systèmes d'information.

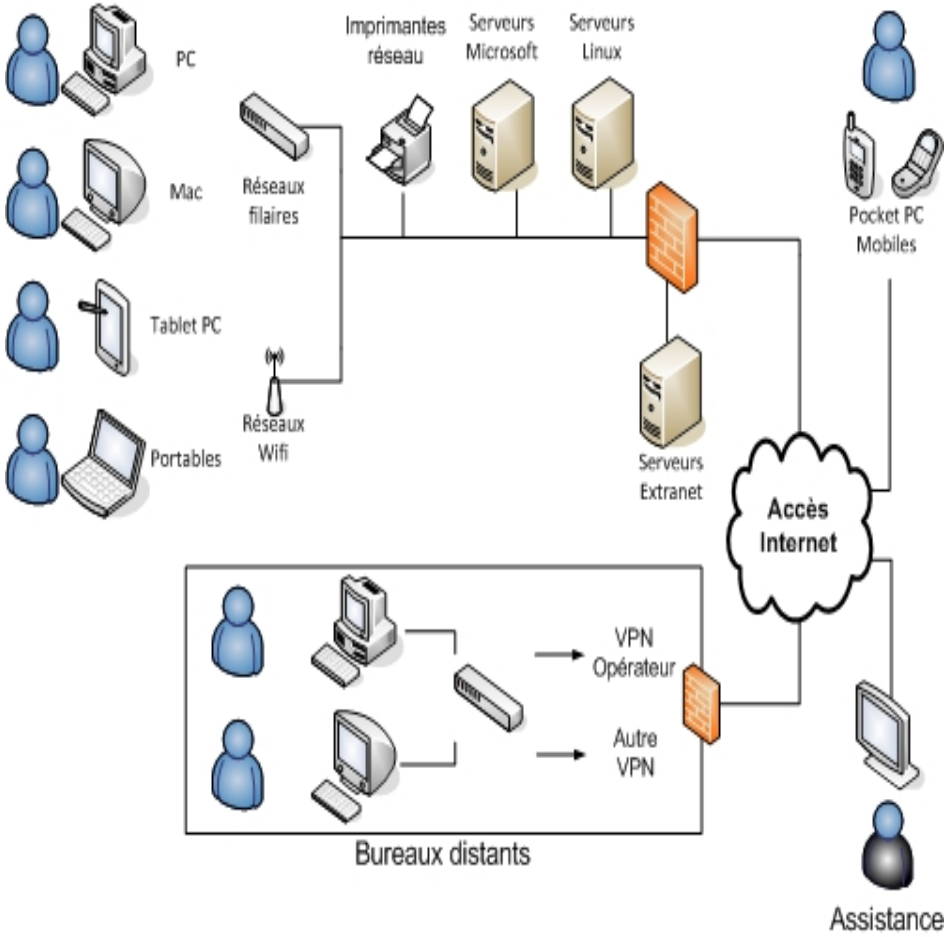
- L'essentiel du système d'information est porté par le système informatique et la notion de sécurité informatique recouvre pour l'essentiel la notion de sécurité des systèmes d'information (SSI).

- Assurer la sécurité de l'information implique l'assurance la sécurité des systèmes informatiques.

- La sécurité informatique :

  La science qui permet de s'assurer que celui qui consulte ou modifie des données du système informatique en a l'autorisation

2. Définitions et concepts de base.



3. Objectifs de la sécurité informatique.

Les principaux objectifs visés par la sécurité informatique sont :

- **Authentification :** vérifier l'identité des personnes qui veulent manipuler l'information.
- **Confidentialité :** L'information ne peut être connue que par les personnes autorisées.
- **Disponibilité :** L'information doit être à la disposition d'un utilisateur qui la demande.
- **Intégrité :** L'information ne doit pas être altérée ou détruite par accident ou par malveillance.
- **Non répudiation :** L'absence de possibilité de contestation (nier) d'une action une fois celle-ci est effectuée.

4. Vulnérabilité.

Définition

Une vulnérabilité(vulnerability) (ou faille) est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte au fonctionnement normal de ce système : à la confidentialité et l'intégrité des données qu'il contient.

- La vulnérabilité représente le niveau d'exposition face à la menace dans un contexte particulier.
- Les vulnérabilités sont la conséquence de défauts dans la conception, la mise en oeuvre ou l'utilisation d'un composant matériel ou logiciel du système.
- On parle aussi de bugs.
- La vulnérabilité concerne tous les composants du système(matériel, logiciel, les règles, les procédures, personnel).

Exemples de vulnérabilités

1. Utilisation des mots de passe non robustes.

2. Présence de comptes non protégés par mot de passe.

3. Dépassement de tampon (en anglais, buffer overflow) est un bug par lequel un processus, lors de l'écriture dans un tampon, écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus.

   - Un bug ("'insecte") ou bogue est un défaut de conception d'un programme informatique à l'origine d'un dysfonctionnement. Ce nom vient du tout premier incident informatique qui a été causé par un insecte.
   - Un bug peut être intentionnel ou non intentionnel.

Principe de fonctionnement du buffer overflow:

Exemples de vulnérabilités

- Les données saisies dans une application sont stockée en RAM dans une zone appelée tampon.
- Un programme doit prévoir une taille maximale pour les données en entrées et vérifier que les données saisies ne dépassent pas cette valeur.
- Les instructions et les données d'un programme en cours d'exécution sont provisoirement stockées en mémoire de manière contiguë dans une appelée pile.
- Les données situées après le tampon contiennent ainsi une adresse de retour (appelée pointeur d'instruction) permettant au programme de continuer son exécution.
- Si la taille des données est supérieure à la taille du tampon, l'adresse de retour est alors écrasée et le programme lira une adresse mémoire invalide.
- Un pirate peut s'assurer que l'adresse mémoire écrasé corresponde à une adresse réelle, par exemple située dans le tampon lui-même. Ainsi, en écrivant des instructions dans le tampon, il lui est simple de l'exécuter.
- Il est ainsi possible d'inclure dans le tampon des instructions ouvrant un interpréteur de commande et permettant au pirate de prendre la main sur le système

4. Une Injection SQL est un type d'exploitation d'une faille de sécurité d'une application interragissant avec une base de données, en injectant une requête SQL non prévue par le système et pouvant compromettre sa sécurité.

Exemple.

- Une requête SQL pour la vérification de mots de passe : `SELECT * from admins WHERE login='$login' AND password='$password'` .
- On peut passer l'identification sans avoir le mot de passe :
  - En tapant un login `'OR 1=1#`, le # étant le caractère de commentaire supprime tout ce qui le suit dans la requête (# ou - - ou /* */).
  - La requête devient `SELECT * from admins WHERE login='' OR 1=1`,
  - `1=1` est une expression toujours vraie, par conséquent cette requête renverra toutes les

5. Le cross-site scripting (abrégé XSS, pour ne pas confondre avec le CSS(Cascading Style Sheet))

- Un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page et de provoquer des actions sur les navigateurs web visitant la page.
- On injecte le code malveillant en langage de script dans un site web vulnérable, par exemple en déposant un message dans un forum qui redirige l'internaute vers un faux site (phishing) ou qui vole vos informations (cookies).
- La faille XSS permet d'exécuter des scripts du coté client. Ceci signifie que vous ne pouvez exécuter que du JAVASCRIPT, HTML et d'autres langages qui ne vont s'exécuter que chez celui qui lance le script et pas sur le serveur directement.

4. Vulnérabilité.

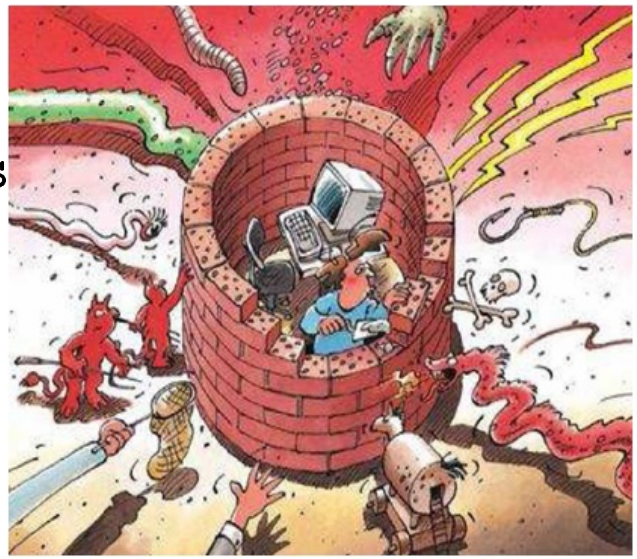
- Les vulnérabilités informatiques proviennent souvent de la négligence ou de l'inexpérience d'un programmeur.

- Une vulnérabilité permet généralement à l'attaquant de duper l'application, par exemple en outrepassant les vérifications de contrôle d'accès ou en exécutant des commandes sur le système hébergeant l'application.

5. Les menaces.

Une menace (threat) représente le type d'action susceptible de nuire au système.
Les menaces sur un SI sont de deux types :

- Menaces accidentels :
  - Panne de disques.
  - Chute de tension.
  - Echange de disques infectés
  - ...
- Menaces intentionnelles :
  - Vol.
  - Ecoute.
  - Fouille.
  - ...



5. Les menaces.

- Le risque en terme de sécurité est généralement caractérisé par l'équation suivante :

$$risque = \frac{(menace * vulnérabilité)}{contremesure}$$

- La contre-mesure est l'ensemble des actions mises en oeuvre en prévention de la menace.

5. Les menaces.

Définition

- *Une attaque est toute action qui compromet la sécurité des informations. C'est la réalisation d'une menace.*
- *Attaque = cible + méthode + Vulnérabilités.*

Les attaques sur les systèmes informatiques sont souvent classés en quatre types :

- Les attaques d'accès.
- Les attaques de modifications.
- Les attaques de saturation (déni de service).
- Les attaques de répudiation.

5. Les menaces.
5.1. Les attaques d'accès.

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information. Il y'a plusieurs exemples, selon la méthode utilisée :

- Ingénierie sociale : L'attaquant établit des relations avec le personnel pour obtenir des informations sur les mots de passe, La topologie du réseau, ...
- Portes dérobées (backdoors) : injecter un code dans la cible pour l'exploiter plus tard.

5. Les menaces.
5.1. Les attaques d'accès.

- **Le Sniffing :** L'attaquant se met à l'écoute sur le réseau pour obtenir des informations.
- **Le Rootkit :** programme permettant de maintenir durablement un accès frauduleux à un système informatique, grâce à des modifications des commandes système et à une porte dérobée difficile de détecter.
- **Le Phishing :** simuler la page Web ou le message d'un tiers de confiance (banque, administration) afin d'extorquer des informations personnelles de l'utilisateur (numéro de carte de crédit, numéro d'état civil, mot de passe etc.).

5. Les menaces.
5.2. Les attaques de modification.

Une attaque de type modification consiste, pour un attaquant à tenter de modifier des informations. Elle est dirigé contre l'intégrité de l'information.

- Virus: un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs.

- Ver : un programme qui se copie lui-même mais qui n'affecte pas d'autres fichiers $\Longrightarrow$ relâcher un ver dans internet permet de ralentir le trafic.

- Bombe logique: un programme qui se déclenche à une date ou à un instant donnée.

- Macro virus: Ils sont insérés dans certains fichiers d'extensions doc, xls, ppt, ... et peuvent exécuter de petis programmes spécifiques sur le document qui les contient.

- cheval de Troie: Un cheval de Troie est un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à l'ordinateur sur lequel il est exécuté en ouvrant une porte dérobée (en anglais backdoor). Il peut
  - voler des mots de passe;
  - copier des données sensibles;
  - exécuter tout autre action nuisible;
  - etc ...

5. Les menaces.
5.3. Les attaques de saturation.

Les attaques par saturation sont des attaques informatiques qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.

- Le flooding: Envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra pas traiter tous les paquets et finira par se déconnecter du réseau.

- Le smurfing: S'appuie sur le ping et les serveurs de broadcast . On falsifie d'abord son adresse IP pour se faire passer pour la machine cible.

- **Le débordement de tampon:** Envoi à la machine cible de données d'une taille supérieure à la capacité d'un paquet. Celui-ci sera alors fractionné pour l'envoi et rassemblé par la machine cible $\Longrightarrow$ il y aura débordement des variables internes.

- **Les spams :** message parasitaire diffusé sur l'Internet dans le but d'encombrer les boîtes aux lettres et le réseau lui-même.

5. Les menaces.
5.4. Les attaques de répudiation.

- Une attaque de répudiation est une attaque contre la responsabilité.

- Elle consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé.

Exemple :

- Le IP spoofing: se faire passer pour une autre machine en falsifiant son adresse IP (Elle est en fait assez complexe).

5. Les menaces.
5.5. Les effets d'une attaque.

- Attaque passive : c'est la moins dangereuse :
  - Ne modifie pas l'information.
  - Consultation de l'information.
- Attaque active : ce type d'attaque est dangereux :
  - Modifie l'état d'une information, d'un serveur ou d'une communication.
  - Connexion frauduleuse à un host ou un réseau.
  - Altération des messages en transit sur un réseau (Denis de service).

6. Les attaquants.

- **Pirate :** celui qui distribue et vend des logiciels protégés sous copyright.

- **Hacker :** Celui qui visite des ordinateurs qui ne lui appartiennent pas sans leurs causer des dommages mais pour personnaliser son système.

- **Cracker :** celui qui veut casser un système et causer des dommages.

- **Les espions:** Pirate payé par une entreprise ou un organisme concurrent pour récolter (de façon frauduleuse) des informations sur un domaine précis.

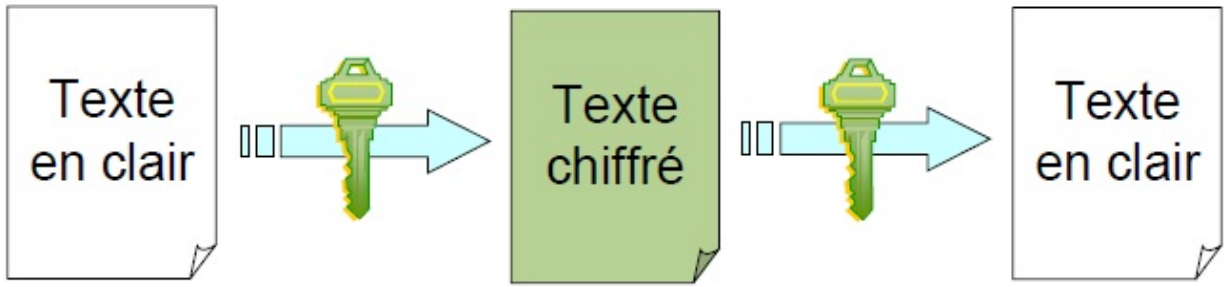
7. Outils de défence.

Les outils de défence les plus courants sont :

- La cryptographie.
- La signature numérique.
- Les firewalls.
- IDS (outil de Détection d'intrusion).
- Serveur Proxy.
- Antivirus.
- Programme de test de vulnérabilité.
- ... .

8. Sécutité par le chiffrement : La cryptographie.

- Art de déssimuler l'information.
- Technique utilisée pour assurer la confidentialité des informations.
- Fondée sur des algorithmes mathématiques pour rendre les données illisibles pour les personnes non autorisées.



- Utilisée lors des échanges des informations ou pour minimiser les dégâts des vols(des ordinateurs portables, des disques, ...)