SÉCURITÉ INFORMATIQUE

L3 systèmes informatiques, 2019/2020

Coefficients et crédits

Unité	Intitulé de la matière	VHS	V.H. Hebdomadaire			Coefficients	Crédits	Mode d'évaluation	
		14-16 Sem	Cours	TD	TP			Continu	Examen
UF3						6	10		
	Applications mobiles	67h30	1h30	1h30	1h30	3	5	50%	50%
	Sécurité informatique	45h	1h30	1h30		3	5	50%	50%

Blog : cryptosdz.blogspot.com

PLAN

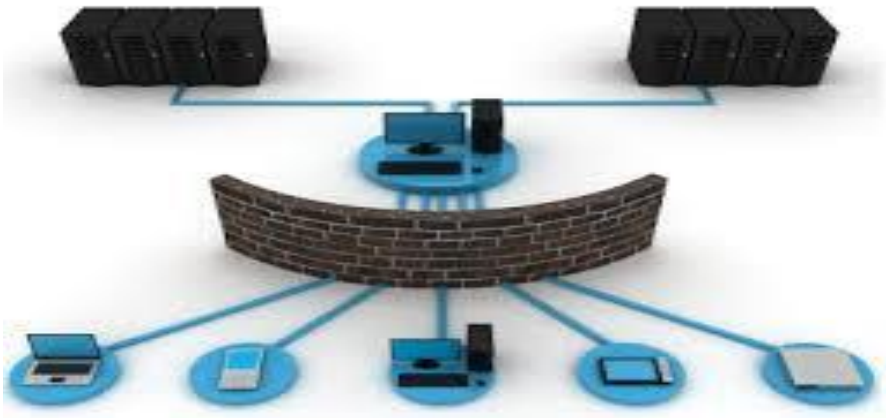
- Introduction à la sécurité
- Chiffrement classique
- Chiffrement moderne
- Fonction de hachage
- Signature digitale
- Cryptanalyse
- Outils de chiffrement
- PKI (Public Key Infrastructure)
- Blockchain

I. INTRODUCTION À LA SÉCURITÉ

- Définition
- Types de menaces
- Services de sécurité
- Mécanismes de sécurité

DÉFINITION

- La sécurité informatique consiste à protéger les ressources matérielles et logicielles contre les risques potentiels (menaces, intrusions,..).
  - Assurer que les ressources matérielles et logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.



TYPES DE MENACES

Menaces accidentelles
Menaces intentionnelles (attaques)

- **Menace accidentelle** : action exécutée par erreur.

Exemples :

- Envoyer des messages publicitaires à quelqu'un peut lui générer un flot de messages inutiles.

- Envoyer un message confidentiel à une mauvaise personne par erreur.

TYPES DE MENACES

Menaces accidentelles
Menaces intentionnelles (attaques)

- **Menace intentionnelle :** action exécutée par une entité pour violer la sécurité :

- *Attaque passive :* permet seulement de collecter des informations en se basant sur les écoutes électroniques.

- *Attaque active :* peut être une destruction, modification, fabrication, interruption ou interception de données.

EXEMPLES D'ATTAQUES

- *Recevoir des messages anonymes :*

(Les messages indésirables (spam), etc…)

- *Attaques contre la confidentialité ou l'intégrité :*

(Le contenu peut être lu ou modifié durant le transfert.)

- *Les accès non autorisés au système de messagerie :*

(détourner le contrôle d'accès, Deviner ou voler un mot de passe.)

- *Usurpation d'identité :*

(Envoi de messages en utilisant l'identité d'autres personnes.)

- Répudiation :

(Nier l'envoi ou la réception de certains messages.)

- Attaque contre la disponibilité :

(Bombarder un serveur de messagerie (TCP-SYN flooding))

- Attaques logicielles :

(Chevaux de Troie, vers,..)

Types d'attaques logicielles

- *Virus*
- *Vers (worm)*
- *Chevaux de troie (Trojan horse)*

Les virus

- *Def :*

Sont capables de se répliquer, puis de se propager à d'autres ordinateurs en s'insérant dans d'autres programmes ou des documents légitimes appelés « hôtes ».

  - Virus de secteur d'amorçage
  - Virus de fichier
  - Virus de macro
  - Virus de script
- *Exp.:*
  - *Wabbit, Boot,…*

Les vers

- *Def :*

sont capables d'envoyer une copie d'eux-mêmes à d'autres machines.

  - Vers de courrier électronique
  - Vers d'Internet
  - Vers IRC (Internet Relay Chats)
  - Vers de réseau

- *Exp.:*
  - *Loveletter (*ILOVEYOU*), Here you have,…*

Les chevaux de troie

- *Def :*

C'est un logiciel malveillant (malware). Un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante.

  - Portes dérobées (back-door)
  - Injeceteurs (Droppers)
  - Notificateurs (Trojan),
  - Logiciels espions (keyloggers)

SERVICES DE SÉCURITÉ

- Confidentialité

rendre la lecture de l'information inintelligible à des tiers non autorisés

- Authentification

identifier l'auteur d'un message

- Intégrité des données

protéger les messages contre toute forme de modification

- Non répudiation

garantir l'authenticité de l'acte

- Contrôle d'accès

limiter et contrôler l'accès aux différentes ressources

MÉCANISMES DE SÉCURITÉ

- **Prévention**

prévenir une violation dans la sécurité (e.g : contrôle d'accès)

- **Détection**

détecter toutes les tentatives de violation de la sécurité

- **Recouvrement**

restaurer l'état du système avant qu'il y est eu violation