UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

Sécurité des Systèmes d'Information (SSI)

Stockage

Dr. C. M. BENTAOUZA

chahinez.bentaouza@univ-mosta.dz

https://sites.google.com/view/cours-bentaouza/accueil

Supports de Stockage

Introduction

- *Les supports de stockage informatique on beaucoup évolués ces dernières années.*

- *Les unités de mesure sont :*

Le kilo-octet (ko) = 1 000 octets
Le méga-octet (Mo) = 1 000 ko
Le giga-octet (Go) = 1 000 Mo
Le téra-octet (To) = 1000 Go

Disquette

- La disquette 3 ½ pouce peuvent stocker 1.44 Mo.

- Elle a été lancée par IBM en 1697 en 8 pouces.
- En 1978, une version plus petite 5 ¼ pouce.
- En 1984, Apple lance une plus petite 3 ½ pouce.

NB:

- Ils ont disparu à cause de leur faible espace de stockage.

CD Rom

- Il a été inventé par Philips en 1979 puis en audio en 1982 pour stocker les données.
- Sa capacité est de 700 Mo pour CD R et 650 Mo pour CD RW

NB:

- R read
- RW read write

DVD Rom

- Il a été lancé en 1995 pour stocker des données.
- Sa capacité est de 4,7 Go en simple couche et 8,5 Go en double couche.

NB:

- Blu-Ray de 25 à 128 Go pour le stockage des films en 3D
- HVD de capacité 3,9 To

Disque dur

- Il a été inventé en 1956 pour stocker des données sous forme de fichiers et dossiers.
- Leurs capacités est de 250 Go à 3 To
- Ils tournent à une vitesse de 7200 tours/minutes.

NB:

- Plus le disque tourne vite moins le temps d'accès sera long.

SSD

- Solid State Drive, lecteur à l'état solide
- C'est une unité de stockage constituée d'une mémoire flash.
- Sa capacité va de 32 Go à 2 To.

NB:

- Avantage : silence de fonctionnement + vitesse à des milliers de tours par minute+ pas de mécanique + faible consommation électrique + résistant aux chocs
- Inconvénient : prix

Carte mémoire

- Elle permet de transférer des données entre appareils.
- Les appellations sont : MS, SD, MMC, SM.
- Leurs capacités actuelles sont de 2 Go, 8 Go à 2 To

NB:

- La carte SD de 512 Mo est compatible avec tous les appareils

Clé USB

- C'est un petit support de stockage qui se branche sur un port USB.
- Sa capacité est de 1 Go à 256 Go.
- Elle est pratique pour transférer des données entre ordinateurs sans installer un programme.

NB:

- Certains intègre un mot de passe comme moyen de sécurité.

Autres supports

- **Lecteur Zip** avec une capacité de 750 Mo
- **Lecteur REV** est actuellement le plus répandu avec une capacité de stockage de 75 Go.
- **Lecteur de bande magnétique** utilisé par l'armé ou les grandes surfaces.

La clé USB du futur peut stocker
360 To de donnés pendant
14 milliards d'années

Disque dur de Quartz 5d de 360 To

Microsoft voit le futur du stockage
des données… dans notre ADN

Capacités de stockage XXL !!!

Partitionnement

Définition de partitionnement

- C'est le partage d'un **support de stockage** en unités distinctes.

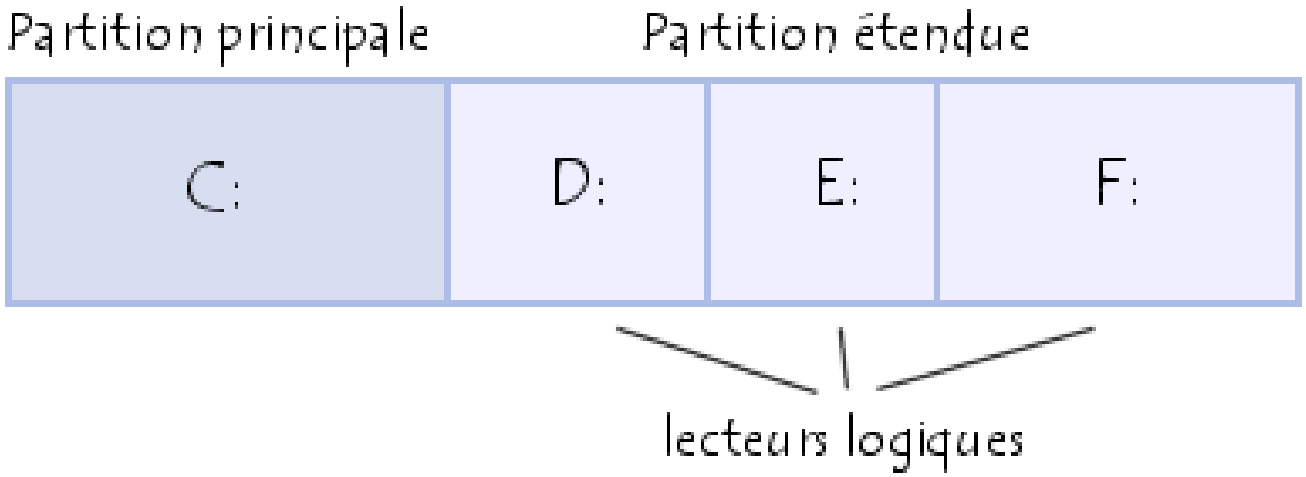
- Elle est utilisée en informatique, où cette expression fait référence à la **partition** d'un **disque dur**, c'est-à-dire à l'une de ses parties dont on **diminue** le **volume**, le plus souvent dans le but de **créer** une autre **partition**.

Objectif de partition

- Installer plusieurs systèmes d'exploitation sur le disque n'utilisant pas le même système de fichiers
- Organiser les données plus facilement en créant **plusieurs lecteurs** dont les données sont séparées.
- Économiser de l'espace disque
- Augmenter la **sécurité** de des fichiers

Type de partition

- La partition principale
  - Elle doit être formatée logiquement, puis contenir un système de fichier correspondant au système d'exploitation installé sur cette partition.
- La partition étendue
  - Elle a été mise au point pour outrepasser la limite des quatre partitions principales, en ayant la possibilité de créer autant de lecteurs logiques cette partition.
- Les lecteurs logiques
  - C'est l'impression qu'on ait plusieurs disques durs de taille inférieur.


Partition principale
Partition étendue
C:
D:
E:
F:
lecteurs logiques

NB:

- Un disque peut contenir jusqu'à :
  - Quatre partitions principales
    - Dont une seule peut être active et visible,
  - Ou trois partitions principales et une partition étendue.
- Au moins un lecteur logique est nécessaire dans une partition étendue.

Table de partitions

- Les informations sur les partitions sont conservées sur le disque dans des zones appelées tables de partitions *(partition map)*.
- La table de partitions principale est contenue dans le premier secteur du disque ou secteur d'amorçage (MBR ou GPT) qui contient le programme d'amorçage.

- **NB:**
  - Chaque ligne d'une table de partitions contient l'adresse de début de la partition et sa taille.

MBR

- Le **secteur de démarrage** (appelé **Master Boot Record** ou **MBR** en anglais) est le premier secteur d'un disque dur (cylindre 0, tête 0 et secteur 1).
- Il contient la **table de partition principale** (*partition table*) et le code, appelé **boot loader**, qui, une fois chargé en mémoire, va permettre d'amorcer (*booter*) le système.

- **NB :**
  - Ce secteur est le plus important du disque dur, il sert au setup du BIOS à reconnaître le disque dur.
  - Sans lui, le disque dur est inutilisable, c'est une cible de prédilection pour les virus.

GPT

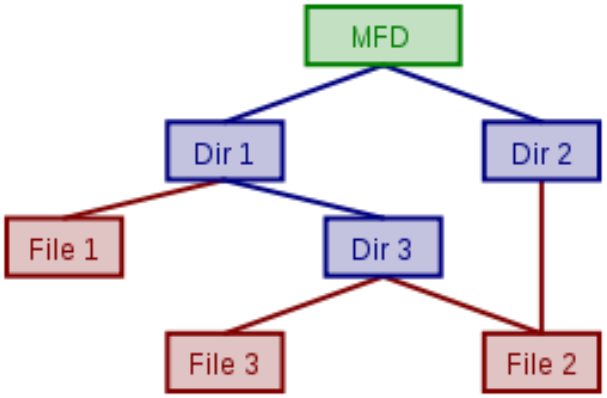
- C'est une **table de partitionnement GUID**, en anglais ***GUID Partition Table*** (GPT) est un standard pour décrire la table de partitionnement d'un disque dur.

- NB :
  - Il est utilisé sur certains BIOS à cause des limitations de la table de partitionnement du MBR.

Système de fichiers

Système de fichier

- Un système de fichiers (« FS » pour File System en anglais) ou système de gestion de fichiers (SGF) est une façon de stocker les informations et de les organiser dans des fichiers sur des supports de stockage.



Fonctions d'un SGF

- Manipulation des fichiers;
- Allocation de la place sur mémoires secondaires;
- Localisation des fichiers;

- Sécurité et contrôle des fichiers :
  - Il permet le partage des fichiers par différents programmes d'applications tout en assurant la sécurité et la confidentialité des données.
  - Donc, un nom et une clé de protection sont associés à chaque fichier afin de le protéger contre tout accès non autorisé ou mal intentionné lors du partage des fichiers.
  - Le SGF se doit aussi de garantir la conservation des fichiers en cas de panne du matériel ou du logiciel.

Système de fichiers et système d'exploitation

- Le choix du système de fichiers se fait en premier lieu suivant le système d'exploitation.

- **NB :**
  - Plus le système d'exploitation est récent plus le nombre de systèmes de fichiers supportés sera important.

Exemples de système de fichiers

- **FAT** : c'est une **table d'allocation de fichiers** (en anglais *FAT*, *File Allocation Table*).
- **NTFS** : c'est un système de fichiers développé par Microsoft Corporation pour sa famille de systèmes d'exploitation (New Technology File System).
- **EXT** : c'est le premier système de fichiers créé en avril 1992 spécifiquement pour le système d'exploitation Linux (**extended file system)**.

Système d'exploitation	Types de système de fichiers supportés
Dos	FAT16
Windows 95	FAT16
Windows 95 OSR2	FAT16, FAT32
Windows 98	FAT16, FAT32
Windows NT4	FAT, NTFS (version 4)
Windows 2000/XP	FAT, FAT16, FAT32, NTFS (versions 4 et 5)
Linux	Ext2, Ext3, ReiserFS, Linux Swap(, FAT16, FAT32, NTFS)
MacOS	HFS (Hierarchical File System), MFS (Macintosh File System)
OS/2	HPFS (High Performance File System)
SGI IRIX	XFS
FreeBSD, OpenBSD	UFS (Unix File System)
Sun Solaris	UFS (Unix File System)
IBM AIX	JFS (Journaled File System)

Système de droits

Droit d'accès

- Le droit sur un fichier permet de limiter les accès à une information dans un base de données, droit d'administration, serveur informatique ou outils de sécurité comme FW, suivant un certain nombre de paramètres.

- NB:
  - C'est une base de la sécurité informatique

Droits de fichier

- Les trois principaux droits sur des fichiers sont :
  - la lecture
    - r
  - l'écriture
    - w
  - l'exécution
    - x

- L'exécution d'un fichier correspond :
  - pour un programme : à son exécution, son lancement
  - pour un répertoire : à y entrer

Permission Unix

- Unix est un système multiutilisateurs.
  - Donc, plusieurs personnes peuvent travailler simultanément sur le même OS.
- Puisque plusieurs utilisateurs peuvent être connectés en même temps.
  - Donc, avoir une excellente organisation dès le départ.
  - Ainsi, chaque personne a son propre compte utilisateur.
  - De ce fait, il existe un ensemble de règles qui disent qui a le droit de faire quoi.

Droits d'Unix

- Les droits sont associés à trois types d'utilisateurs :
  - le propriétaire du fichier
    - u
  - les utilisateurs appartenant au groupe auquel appartient le fichier
    - g
  - tous les autres utilisateurs
    - o

- NB:
  - Seuls *root* et le propriétaire d'un fichier peuvent changer ses permissions d'accès.

    - Lorsque le droit n'est pas attribué, on écrit un tiret « - »

Représentation des droits

```
rwxr-xr--
\ /\ /\ /
 v  v  v
 |  |  droits des autres utilisateurs (o)
 |  |
 |  droits des utilisateurs appartenant au groupe (g)
 |
droits du propriétaire (u)
```

Définition privilège

- C'est un avantage exclusif, droit particulier, accordé à quelqu'unou à une certaine catégorie de population.

NB:

- passe-droit

Attribution des privilèges

- Ils sont attribuer à :
  - Utilisateur spécifique
    - Administrateur
    - Modérateur
  - Groupe d'users
    - Membre d'un département

Gestion des privilèges

- Elle se fait selon :
  - Groupe de travail (Workgroups)
  - Groupe résidentiel
  - Domaines spécifiques aux serveurs réseaux

Exemple SQL

Classes de privilèges	Types de compte
accès au contenu de l'information	utilisateur, application
gestion du schéma de la base de données	administrateur, application (parfois)
gestion des privilèges utilisateurs	administrateur
gestion des paramètres systèmes	administrateur

Redondance

Redundancy

Définition

- En informatique et dans les télécommunications, duplication d'informations afin de :
  - Garantir leur sécurité en cas d'incident (Larousse)
  - Corriger des erreurs de transmissions pour assurer la fiabilité
    - code correcteur
  - Détecter les erreurs
    - somme de contrôle
  - Assurer un fonctionnement sans interruption en cas de dysfonctionnement du premier, le second en reprend le relais
- NB:
  - La compression de données permet de réduire ou d'éliminer la redondance que l'utilisateur ne désire pas conserver

Contrôle par redondance

- Un **contrôle par redondance** consiste à ajouter des données à la fin d'un message pour détecter des erreurs et éventuellement les corriger.
- N'importe quelle fonction de hachage comme MD5 peut être utilisée en tant que contrôle par redondance.
- Les plus simples sont les sommes de contrôle, incluant le bit de parité. On trouve également d'autres contrôles par redondance : le CRC (*Cyclic Redundancy Check) ou (*Contrôle de redondance cyclique)

Code correcteur

On présente ici un exemple élémentaire de code correcteur obtenu en complétant une suite de trois nombres (constituant l'information à transmettre) par deux autres nombres (constituant le code de contrôle de l'information). L'ensemble des cinq nombres permet alors de détecter et de corriger une erreur qui se serait produite sur l'un des trois premiers nombre lors de la transmission.

Soit donc un bloc de 3 nombres que l'on souhaite transmettre : 02 09 12

Ajoutons deux nombres de contrôle de l'information.
Le premier est la somme des 3 nombres : 02 + 09 + 12 = 23
Le second est la somme pondérée des 3 nombres, chacun est multiplié par son rang : 02x1 + 09x2 + 12x3 = 56
À la sortie du codeur, le bloc à transmettre est : 02 09 12 23 56

À la suite d'une perturbation, le récepteur reçoit : 02 **13** 12 23 56

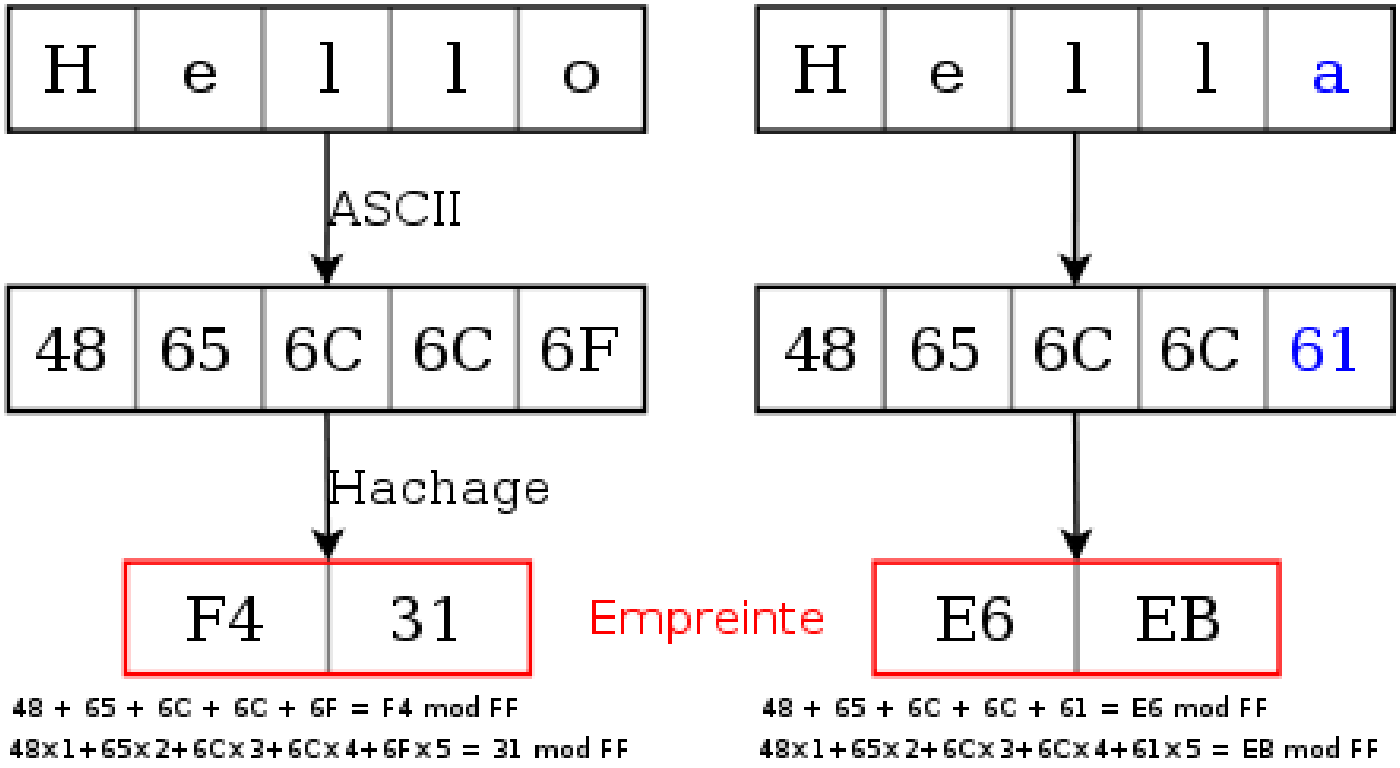
À partir des données reçues, le décodeur calcule :
Sa somme simple : 02 + **13** + 12 = **27**
Sa somme pondérée : 02x1 + **13**x2 + 12x3 = **64**

La différence entre la somme simple calculée (**27**) et celle reçue (23) indique la valeur de l'erreur : 4 (**27**-23 = 4)
La différence entre la somme pondérée calculée (**64**) et celle reçue (56), elle-même divisée par la valeur de l'erreur indique la position où l'erreur se trouve : 2 ((**64**-56) / 4 = 2).
Il faut donc retirer 4 au nombre du rang 2.

Le bloc original est donc 02 (**13**-4=09) 12 23 56

Lors d'une transmission sans perturbation, les différences des sommes simples et des sommes pondérées sont nulles.

Somme de contrôle



KEEP
CALM
AND
DO YOUR
BEST