Université des sciences et de la Technologie Houari Boumediene
USTHB – Alger

Département d'Informatique

MASTER SYSTÈMES INFORMATIQUES INTELLIGENTS

MASTER INFORMATIQUE VISUELLE

MASTER ARCHITECTURES PARALLÈLES ET CALCUL INTENSIF

ARCHITECTURE ET ADMINISTRATION DES BASES DE DONNÉES

2016-2017

ENSEIGNANT : M. KAMEL BOUKHALFA

SÉCURITÉ DES BASES DE DONNÉES

CONÇUS PAR :
Z. ALIMAZIGHI, K. BOUKHALFA

INTRODUCTION

- Les données constituent une ressource essentielle et stratégique pour une organisation qui doivent donc demeurer confidentielles et en sécurité.
- La sécurité est la protection de la base de données contre les accès mal intentionnés ou accidentels.

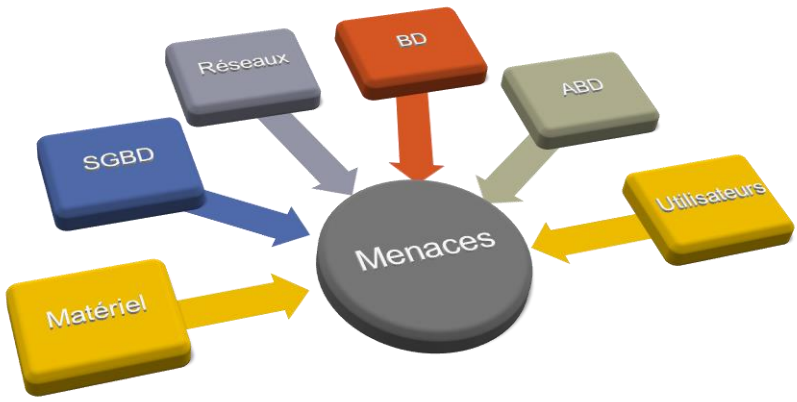
INTRODUCTION

- **Comme pour la gestion de transactions, il va exister une granularité de l'objet à protéger:**
  - BD entière
  - Une relation
  - Une page
  - Un champ.

CONCEPTS GÉNÉRAUX

- **Définition :** la sécurité d'une BD est un ensemble de mécanismes de protection de la BD contre les menaces accidentelles ou intentionnelles
- Une menace est toute situation ou tout événement intentionnel ou accidentel, qui risque de porter atteinte à un système et donc à l'organisation entière
- **Exemples**
  - Vol, fraude
  - Perte de la confidentialité
  - Les atteintes à la vie privée
  - La perte d'intégrité, la perte de disponibilité

MENACES POTENTIELLES À L'ENCONTRE DES SYSTÈMES INFORMATIQUES



MENACES POTENTIELLES

- **Matériels**
  - Incendie, inondation, échec des mécanismes de sécurité, vol d'équipement etc.
- **SGBD et logiciels d'application**
  - Echec des mécanismes de sécurité donnant un accès plus étendu que normalement, altération des programmes etc.
- **Réseaux de communication**
  - Branchement et écoute illicite
  - Coupure de câbles etc.

MENACES POTENTIELLES

- **Bases de données**
  - Modification ou copie non autorisée
  - Vol de données, etc.
- **Administrateur de la base de données**
  - Stratégies et procédures de sécurité inadéquates
- **Utilisateurs**
  - Utilisation par une personne non autorisée, entrée illégale d'un pirate etc.

CONTRE-MESURES
LES CONTRÔLES INFORMATIQUES

- **Le type de contre-mesure vont des contrôles physiques aux procédures administratives.**
- **Les contrôles**
  - Les autorisations
  - Les vues
  - Les sauvegardes et restaurations
  - L'intégrité
  - Le cryptage

LES AUTORISATIONS

- **Une autorisation**
  - Attribution d'un droit ou d'un privilège qui permet à un sujet de disposer légitimement d'un accès à un système ou à un objet d'un système.
- **Une authentification est le mécanisme qui détermine si un utilisateur est celui ou celle qu'il ou qu'elle prétend être**

LES CONTRÔLES D'ACCÈS

- Le contrôle d'accès repose sur l'attribution et la révocation de privilèges
- Un privilège permet à un utilisateur de créer (écrire et modifier) un objet d'une BD, ou d'y accéder (lecture).
- Les SGBD fournissent deux catégories d'approches de contrôle d'accès:
  - **Contrôle discrétionnaire :** basé sur l'utilisateur et sur les privilèges ou autorisations
  - **Contrôle obligatoire :** marquage de la donnée avec un niveau de classification

CONTRÔLES D'ACCÈS

- **Contrôle discrétionnaire**
  - Un utilisateur donné aura différents droits d'accès sur différents objets; des utilisateurs différents pourront avoir des droits différents sur le même objet
- **Contrôle obligatoire**
  - Chaque objet est marqué avec un niveau de classification et à chaque utilisateur est attribué un niveau d'habilitation
- **Remarque**
  - Dans la deuxième approche, un objet donné ne peut être accédé que si l'utilisateur a le niveau d'habilitation approprié, elle est donc plus rigide que l'approche discrétionnaire

CONTRÔLES D'ACCÈS

- Les règles d'autorisation doivent être sauvegardées dans un catalogue
- Une demande d'accès doit pouvoir être testée pour savoir si elle répond à la règle de sécurité:
  - Existence d'un sous-système de sécurité dans le SGBD appelé sous-système d'autorisation
- Il faut que le système soit capable de détecter quelle règle doit être associé à une demande, pour cela il faut une authentification du demandeur à travers une identification et un mot de passe
- Il faut un langage pour pouvoir décrire les règles d'autorisation : SQL

LES CONTRÔLES D'ACCÈS DISCRÉTIONNAIRES

- Gestion en SQL des privilèges grâce aux commandes :

  GRANT(accorder) et REVOKE (révoquer)

  GRANT (liste privilège/ ALL PRIVILEGES)

  ON Nom objet

  TO (liste autorisations/ PUBLIC)

  [WITH GRANT OPTION]

CONTRÔLE D'ACCÈS DISCRÉTIONNAIRE

- **Liste de privilèges :**
  - SELECT, DELETE, INSERT, UPDATE,
- **Nom objet** : nom de table, d'une vue, d'un domaine
- **WITH GRANT OPTION :** transmet à d'autres utilisateurs de la liste les privilèges reçus

EXEMPLES

Accorder à l'utilisateur dont l'identification est *directeur* tous les privilèges sur la table *personnel.*

GRANT ALL PRIVILEGES

ON personnel

TO directeur

EXEMPLES

Accorder aux utilisateurs sous-directeur et chef-service les privilèges SELECT et UPDATE sur la colonne salaire de la table personnel

GRANT SELECT, UPDATE(salaire)
ON personnel
TO sous-directeur, chef-service

EXEMPLES

- Accorder à tous les utilisateurs le privilège SELECT sur la table grille-salaire

GRANT SELECT

ON grille-salaire

TO PUBLIC

RETIRER UN PRIVILÈGE

REVOKE [GRANT OPTION FOR] (liste de privilèges/ ALL PRIVILEGES]

ON nom objet

FROM (liste autorisations/ PUBLIC) [RESTRICT/CASCADE]

- **Si un utilisateur A donne un certain privilège à un utilisateur B, A peut aussi révoquer ce privilège:**
  - **GRANT OPTION FOR** : permet de supprimer tous les privilèges transmis par la clause **WITH GRANT OPTION**
- **ALL PRIVILEGES** : références à tous les privilèges accordés à un utilisateur

RESTRICT ET CASCADE

- Supposons p un privilège, A accorde p à B, qui à son tour l'accorde à C
- **Si A révoque p à B**
  - **RESTRICT** : le privilège p détenu par C n'est pas abandonné.
  - **CASCADE**: le privilège p détenu par C doit être abandonné.
- **Remarque :**
  - Si le privilège p est aussi transmis par un autre utilisateur D à C alors, il peut garder celui-ci.

EXEMPLES

- Retirer à tous les utilisateurs le privilège SELECT sur la table grille-salaire

```
REVOKE SELECT
ON grille-salaire
FROM PUBLIC
```

- Retirer à l'utilisateur chef-service tous les privilèges accordés sur la table personnel

```
REVOKE ALL PRIVILEGES
ON personnel
FROM chef-service
```

CONTRÔLE D'ACCÈS OBLIGATOIRE

- **Cette approche se base sur l'utilisation d'une échelle de sécurité**
  - Par exemple quatre classes de sécurité
    - Très secret (TS)
    - Secret (S)
    - Confidentiel (C)
    - Universel (U)
  - TS>S>C>U
- **Chaque objet de la BD reçoit une classe de sécurité.**
- **Tout utilisateur reçoit une autorisation d'utilisation d'une classe de sécurité**
- **Des règles s'appliquent à la lecture et écriture dans ces objets par les utilisateurs**

CONTRÔLE D'ACCÈS OBLIGATOIRE

- **Deux règles doivent être respectées**
  - **Règle 1** : le sujet X est autorisé à lire un objet O ssi **classe(X) >=classe(O)**
  - *Si classe (X) = TS, alors X peut lire un objet O avec classe(O) = C, l'inverse n'est pas vrai*
  - **Règle 2:** le sujet X est autorisé à écrire dans l'objet O ssi **classe(X) = classe(O)**
  - un sujet X de classe S ne peut écrire que sur des objets classés S .

CHIFFREMENT (CRYPTAGE) DES DONNÉES

- Tout ce qui vient d'être vu se base sur l'utilisation normale du système
- Si un utilisateur essaye de contourner le système d'autres contre-mesures sont nécessaires comme le cryptage des données
- **Le cryptage** est un codage des données suivant un algorithme spécifique qui rend les données illisibles par tout programme ne disposant pas de la clé de cryptage

CHIFFREMENT (CRYPTAGE) DES DONNÉES

- **Un système de cryptage comporte**
  - Une clé de cryptage
  - Un algorithme de cryptage qui en fonction de la clé de cryptage transforme un texte en clair en un texte crypté
  - Une clé de décryptage pour déchiffrer le texte crypté
  - Un algorithme de décryptage qui, selon la clé de décryptage transforme le texte crypté en texte en clair