Méthodologie de la sécurité informatique

(Contrôle d’accès dans les bases de données)

Introduction

- Les bases de données fournissent un bon moyen d'organisation et de stockage des données
  - ✓ Stockage fiable
  - ✓ Possibilité de stockage à distant
  - ✓ Accès rapide aux données

- Sécuriser une base de données signifie assurer 3 objectifs:
  - ✓ Confidentialité: protection contre la divulgation non autorisée des données
  - ✓ Intégrité: protection contre la modification non autorisée des données
  - ✓ Disponibilité: fournir les données au utilisateurs autorisés selon le besoin

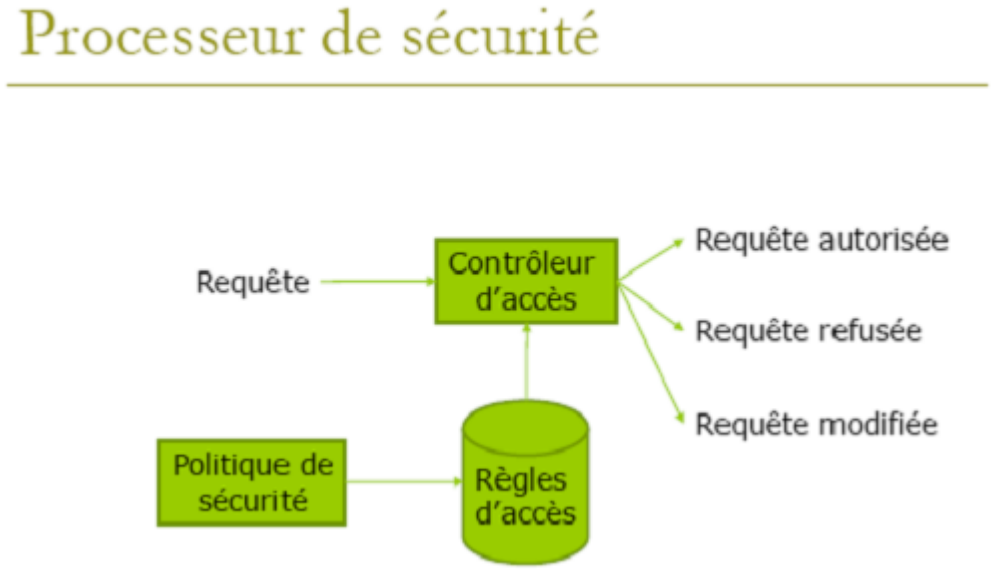
- Mais le problème qui se pose et la sécurisation de ces données
  - ✓ La sécurité est la dernière chose que les administrateur pensent
  - ✓ La politique de sécurisation permet de fuir les données?

Problématiques majeures

- Comment peut-on protéger les données ?
  - Par sécurisation des données elle-même
  - Par sécurisation des accès
  - Par combinaison de plusieurs méthodes

- Quels sont les objets ciblés?
  - BDD
  - Table dans BDD
  - Attributs d'une table (vue)

SGBD et contrôle d'accès



- Basé sur modèle DAC et RBAC
- Sujets : utilisateurs, groupe d'utilisateurs, tous les utilisateurs
- Objets: BD, tables, vues, index, procédures, · · ·
- Privilèges: sur les tables, sur le schéma, sur la base de données
- Rôles: groupe de privilèges

SGBD et contrôle d'accès

Différentes politiques d'implémentation

- Politique (administration) centralisée:
  - ✓ Un nombre spécifique d'utilisateurs peuvent définir les droits d'accès
- Politique basée sur propriétaire
  - ✓ Seul le propriétaire de la BDD peut définir les droits d'accès
- Politique décentralisée
  - ✓ Le propriétaire de la BDD peut définir des droits d'accès a d'autres utilisateurs qui peuvent à leur tour définir les droits à d'autres sur la même BDD

SGBD et contrôle d'accès

Requêtes SQL pour contrôle d'accès

❖ attribution de privilèges sur des objets oracle

GRANT liste-droits | ALL ON nom-composant TO liste-utilisateurs | PUBLIC [WITH GRANT OPTION] ;

- ❖ **ALL :** tous les privilèges que le donneur peut accorder
- ❖ **PUBLIC :** tous les utilisateurs connus du système
- ❖ **WITH GRANT OPTION** : possibilité de transmettre les privilèges qui lui sont accordés

❖ suppression de privilèges sur des objets oracle

REVOKE [GRANT OPTION FOR] liste-droits | ALL ON nom-composant FROM liste-utilisateurs | PUBLIC [RESTRICT | CASCADE] ;

- ❖ **CASCADE :** révocation concerne les utilisateurs cités dans la clause FROM ainsi que ceux `a qui les privilèges ont été récursivement transmis
- ❖ **RESTRICT:** révocation concerne les utilisateurs cités dans la clause FROM
- ❖ **[GRANT OPTION FOR]** pas les privilèges révoqués mais le droit de les transmettre

SGBD et contrôle d’accès

Graphe d’octroi des privilèges

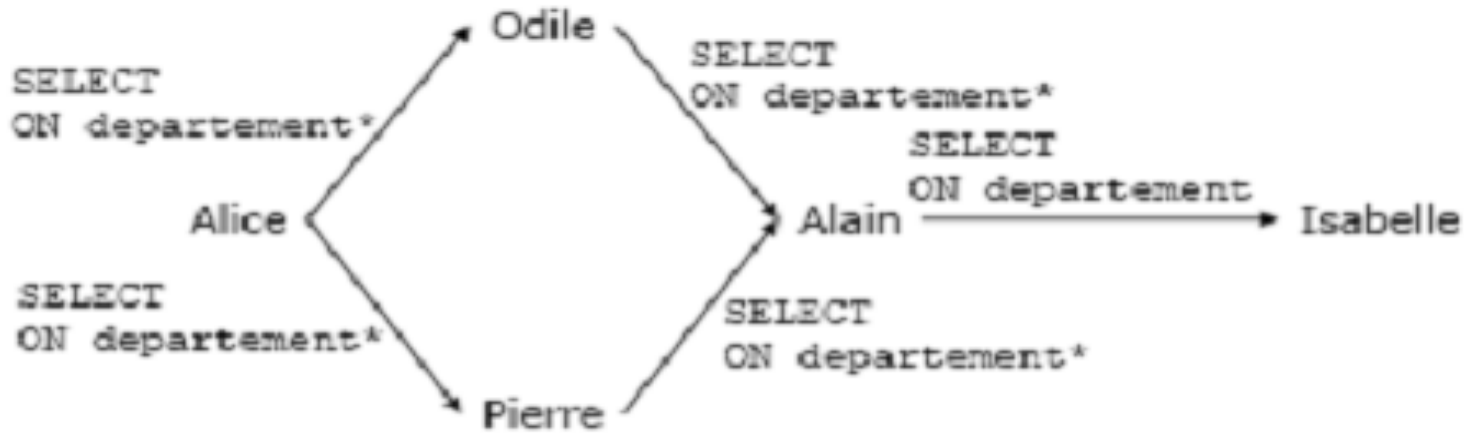
- ✓ Un moyen de présentation graphique d’octroi des privilèges
- ✓ Permet de détecter les failles de sécurité en représentant les chemins et cherchant le chemin le moins sécurisé
- ✓ Chaque nœud représente un utilisateur
- ✓ Chaque arc représente une requête autorisée

SGBD et contrôle d'accès

Graphe d'octroi des privilèges

Octroi de privilèges : exemple

```
Alice    : GRANT SELECT ON departement TO odile WITH GRANT OPTION;
Alice    : GRANT SELECT ON departement TO pierre WITH GRANT OPTION;
Odile    : GRANT SELECT ON departement TO alain WITH GRANT OPTION;
Pierre   : GRANT SELECT ON departement TO alain WITH GRANT OPTION;
Alain    : GRANT SELECT ON departement TO isabelle;
```

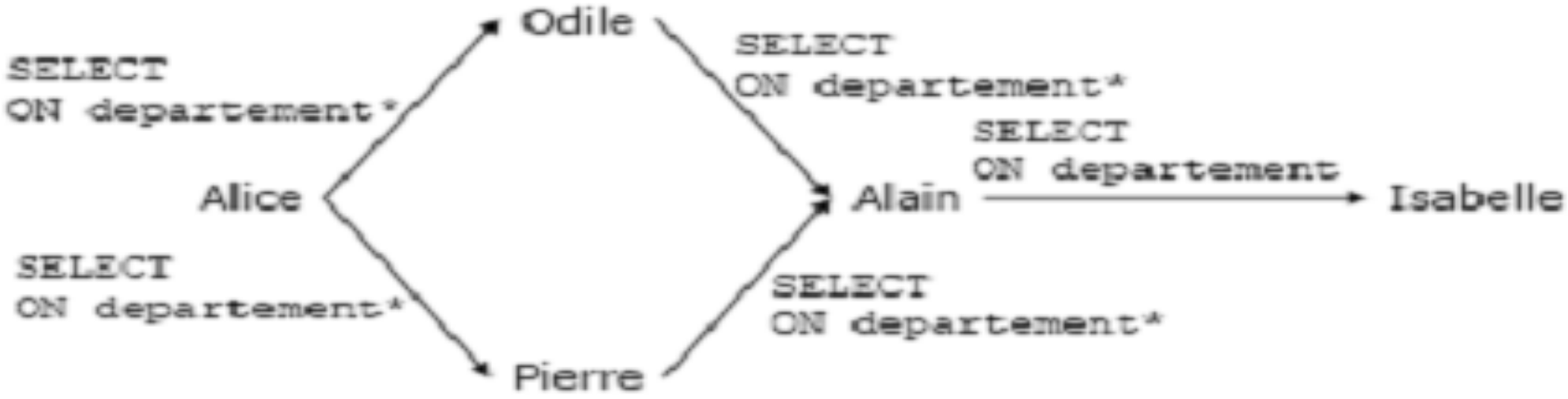


* indique que le privilège a été accordé WITH GRANT OPTION.

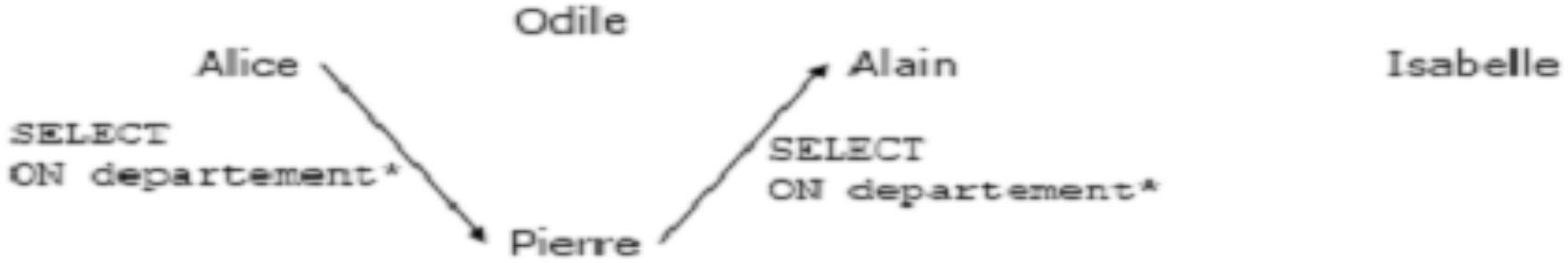
SGBD et contrôle d'accès

Graphe d'octroi des privilèges

Révocation en cascade : exemple



Alice : REVOKE SELECT ON département FROM odile CASCADE



SGBD et contrôle d'accès

Contrôle d'accès sur les attributs: VUE

- elles permettent de définir de façon précise les portions dune BD sur lesquelles des privilèges sont accordés.

exemple table : employe(nom, departement, salaire)

- restriction de l'accès à l'affectation ou au salaire d'un employé en définissant les deux vues suivantes :

```
create view affectation employe(nom, departement) as select nom, departement from employe
create view salaire employe(nom, salaire) as select nom, salaire from employe
```

- et en accordant des priviléges sur chacune de ces deux vues,

```
grant update on salaire employe to Pierre
```

SGBD et contrôle d'accès

Contrôle d'accès sur les attributs: VUE

Exemple : matrice d'accès

	Employé	*Département*	*Affectation*	*Mon_employé*
Alain			SELECT	SELECT
Alice	*tous les privilèges*	*tous les privilèges*	*tous les privilèges*	*tous les privilèges*
Isabelle			SELECT	
Odile	UPDATE(nom_dept)	UPDATE(responsable)	SELECT	
Pierre	UPDATE(salaire)		SELECT	

SGBD et contrôle d'accès

Contrôle d'accès sur les attributs: VUE

Exemple : effets sur les requêtes

	`SELECT * FROM affectation`	`UPDATE employe SET salaire = 2000 WHERE nom = 'isabelle'`	`UPDATE departement SET responsable = 'isabelle' WHERE nom = 'informatique'`
alain	acceptée	refusée	refusée
alice	acceptée	acceptée	acceptée
isabelle	acceptée	refusée	refusée
odile	acceptée	acceptée	acceptée
pierre	acceptée	acceptée	refusée

SGBD et contrôle d’accès

Contrôle d’accès à base de rôles

- Implémenté dans le SGBD **ORACLE**
- Un rôle est un ensemble de privilèges regroupés pour réduire la taille des requêtes
- Le rôle est attribué comme étant un droit aux utilisateurs
- Il peut être un sujet et un droit
- Un rôle ne peut en aucun cas attribuer des droits aux utilisateurs

SGBD et contrôle d'accès

Contrôle d'accès à base de rôles

❖ Création d'un rôle

CREATE ROLE nom_rôle [IDENTIFIED BY mot_de_passe] ;

❖ suppression d'un rôle

DROP ROLE nom_rôle;

❖ Ajouter des droit à un rôle

GRANT liste-droits | ALL ON nom-composant TO nom_role [WITH GRANT OPTION] ;

❖ supprimer des droit d'un rôle

REVOKE [GRANT OPTION FOR] liste-droits | ALL ON nom-composant FROM nom_role
[RESTRICT | CASCADE] ;

SGBD et contrôle d’accès

Contrôle d’accès à base de rôles

❖ Attribuer des rôles à un utilisateur

GRANT liste-rôles TO liste-utilisateurs [WITH ADMIN OPTION] ;

❖ supprimer des rôles d’un utilisateur

REVOKE [GRANT OPTION FOR] liste-rôles FROM liste-utilisateurs [RESTRICT | CASCADE] ;