C018SA-W4-S4

informatiques mathématiques

SEMAINE 4 : Contrôle d'Accès

1. Introduction
2. Modèle de contrôle d'accès discrétionnaire (DAC)
3. Modèle de contrôle d'accès basé sur les rôles (RBAC)
4. **Modèle de contrôle d'accès obligatoire (MAC)**

Les limites de DAC et RBAC

- DAC → l'application s'exécutant pour le compte d'un utilisateur hérite des droits de ce dernier
- RBAC → l'application s'exécutant pour le compte d'un utilisateur hérite des droits associés aux rôles activés dans la session ouverte par ce dernier

→ Risque de programmes malveillants :

- **Cheval de Troie :** programme qui a une fonctionnalité apparente mais qui contient des fonctions cachées
- **Objectif :** transmission illégale d'informations vers le bénéficiaire du piège

Le modèle MAC : une politique de sécurité multi-niveaux

- **Niveaux de sécurité hiérarchiques**
  - *Cloisonnement vertical :* Unclassified < Confidentiel < Secret < Top Secret …
- **Catégories**
  - *Cloisonnement horizontal :* DRH, DAF, etc…
- **Classe d'accès =** combinaison d'un niveau de sécurité et d'une catégorie
  - Le niveau de sécurité d'une classe d'accès associée à un **objet** est appelé *niveau de classification*
  - Le niveau de sécurité d'une classe d'accès associée

  à un **utilisateur** est appelé *niveau d'accréditation*

  (Clearance)

Fonctionnement

- **La décision d'accès est prise en comparant les deux classes d'accès de l'objet et du sujet**
  - *No read up :* un sujet est autorisé à lire un objet seulement si sa classe d'accès domine la classe d'accès de l'objet
  - *No write down :* un sujet est autorisé à écrire un objet seulement si sa classe d'accès est dominée par la classe d'accès de l'objet

- **Une classe d'accès c_1 domine ($\geq$) c_2 ssi :**
  - Le niveau de sécurité de $c_1 \geq$ niveau de sécurité de c_2
  - Les catégories de $c_1 \subseteq c_2$
  - Les deux classes c_1 et c_2 sont dites incomparables ssi $c_1 \geq c_2$ ni $c_2 \geq c_1$ ne sont vérifiées

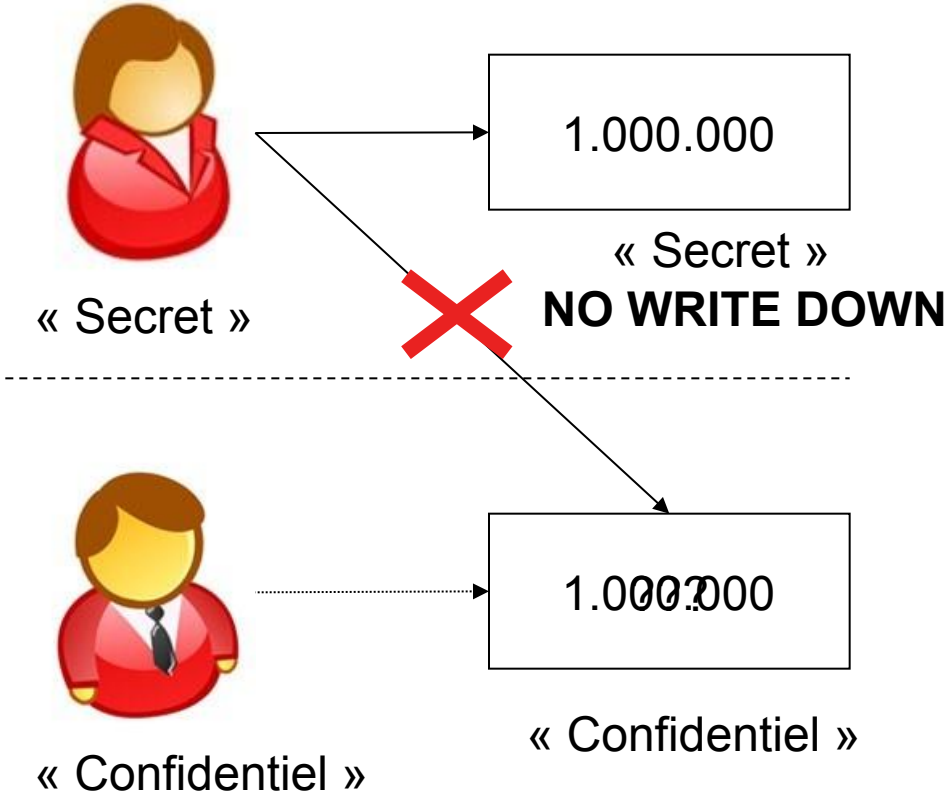
Exemple

- **Données**
  - Le salaire du directeur a un niveau de classification « Secret », et une catégorie « DAF »
  - Le salaire d'un employé a un niveau de classification « Confidentiel », et une catégorie « DAF »

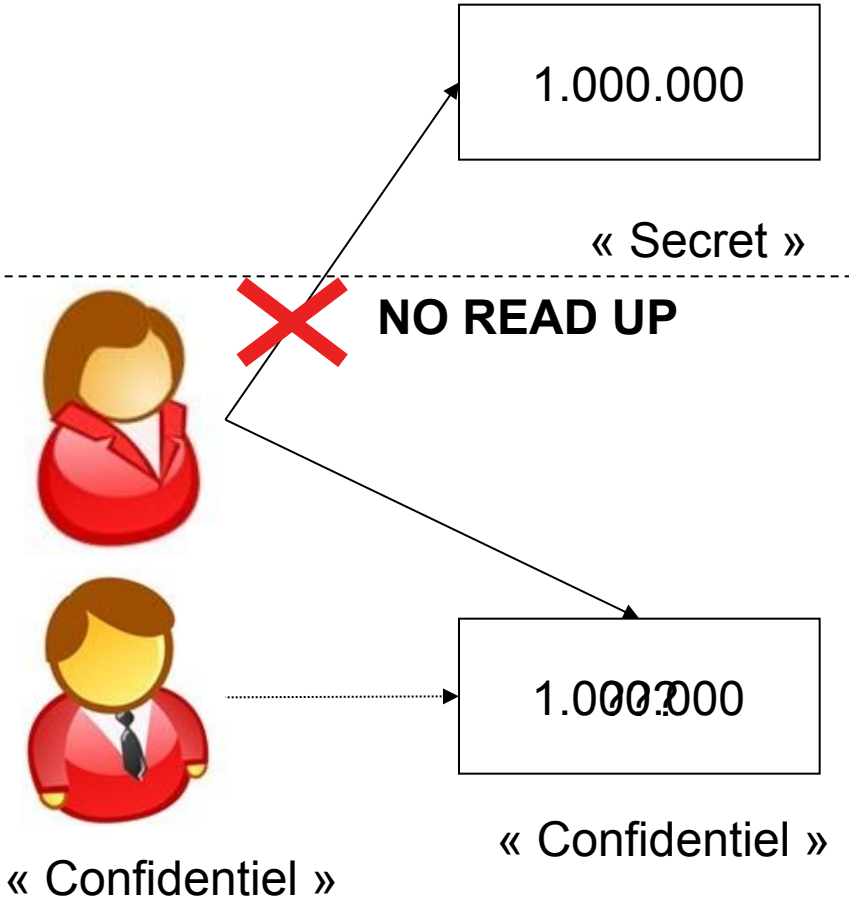
- **Utilisateurs**
  - Alice a un niveau d'accréditation « Secret » et peut accéder à la DAF
  - Bob a un niveau d'accréditation « Confidentiel » et peut accéder à la DAF.

Est-ce qu'Alice peut communiquer le salaire du directeur à Bob ?

Exemple


1.000.000
« Secret »
« Secret »
NO WRITE DOWN
1.000.000
« Confidentiel »
« Confidentiel »

Exemple


1.000.000
« Secret »
NO READ UP
1.000.000
« Confidentiel »
« Confidentiel »

Implémentation : Oracle Label Security
Niveaux de Sécurité

- **Data Label**
  - Constitué de 3 composants (Level, Compartment, Group)
  - Intégré aux nuplets dans une colonne additionnelle (déclarée par le DSA)
  - Valeurs définies par le DSA
- **Level (niveau de sécurité)**
  - Obligatoire, unique, hiérarchique, dénotant la sensibilité de la donnée
  - Exemple: Confidentiel, Secret, Top Secret, etc…
-

Implémentation : Oracle Label Security
Catégories

- **Compartment**
  - Obligatoire, non unique, non hiérarchique, utilisé pour compartimenter les données
  - Exemple: types de données, liste de projets ou de secteur d'activité
- **Group**
  - Optionnel, non unique, potentiellement hiérarchique, utilisé pour isoler les données par organisation
  - Exemple: FBI, CIA, NSA

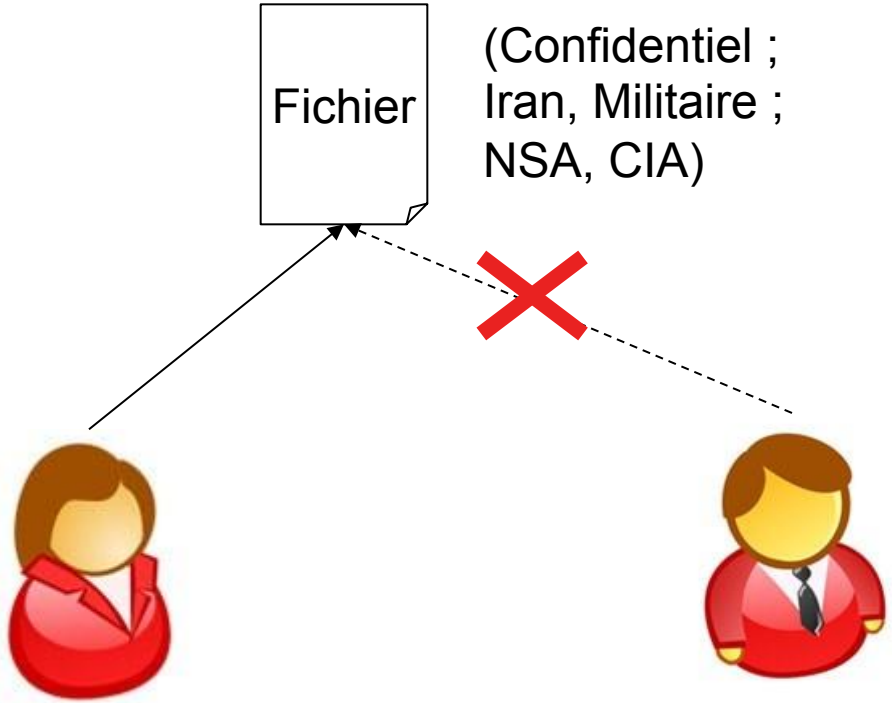
Implémentation : Oracle Label Security
Règles d'accès

Il y a **obligation** de remplir ces règles !

- **Un user label est associé à chaque utilisateur**
  - Mêmes composants: Level, Compartment, Group

- **Autorisations requises pour accéder aux données**
  Les 3 conditions ci-dessous sont requises
  - UserLabel.level ≥ DataLabel.level
  - DataLabel.compartment ⊆ UserLabel.compartment
  - UserLabel.group ⊆ DataLabel.group

Oracle Label Security : Exemple



Conclusion sur le contrôle d'accès

- **Principe Fondateur :**

- **DAC**
  - Structuration des objets
- **RBAC**
  - Structuration des sujets
- **MAC**
  - Lutte contre les programmes malveillants
  - Politiques lourdes et complexes à définir

Tout ceci ne fonctionne que si
l'attaquant passe par la porte d'entrée !