Les modèles de contrôle d'accès sont essentiels pour gérer et restreindre l'accès aux ressources d'un système informatique. Voici un aperçu des principaux modèles de contrôle d'accès : Discretionary Access Control (DAC), Mandatory Access Control (MAC) et Role-Based Access Control (RBAC).

## 1. Discretionary Access Control (DAC)

**Définition**:
Le modèle de contrôle d'accès discrétionnaire (DAC) est un modèle où les propriétaires de ressources ou d'objets ont le pouvoir de décider qui peut accéder à leurs ressources et avec quels privilèges.

**Caractéristiques**:

- **Flexibilité** : Les utilisateurs ont la liberté de partager leurs ressources avec d'autres.
- **Contrôle par l'utilisateur** : Le contrôle d'accès est basé sur les identités des utilisateurs et les permissions définies par les propriétaires des ressources.
- **Permissions basées sur les fichiers** : Les permissions sont souvent gérées par les propriétaires des fichiers et des répertoires.

**Exemple**:
Environnement UNIX/Linux où les propriétaires de fichiers peuvent définir les permissions d'accès pour leurs fichiers en utilisant des commandes comme `chmod`.

```
chmod 755 fichier.txt
```

## 2. Mandatory Access Control (MAC)

**Définition**:
Le modèle de contrôle d'accès obligatoire (MAC) est un modèle où l'accès aux ressources est contrôlé par des politiques de sécurité centralisées définies par l'administration système et non par les propriétaires des ressources.

**Caractéristiques**:

- **Centralisation** : Les décisions d'accès sont prises par un administrateur central et non par les utilisateurs individuels.
- **Labels de sécurité** : Les objets (fichiers, données) et sujets (utilisateurs, processus) sont assignés des labels de sécurité.
- **Politiques strictes** : Les politiques de sécurité sont strictes et non modifiables par les utilisateurs.

**Exemple**:
SElinux (Security-Enhanced Linux) est un exemple de mise en œuvre de MAC où les politiques de sécurité sont définies par l'administrateur et appliquées strictement.

```
sestatus
```

### 3. Role-Based Access Control (RBAC)

**Définition**:
Le modèle de contrôle d'accès basé sur les rôles (RBAC) est un modèle où les permissions sont associées à des rôles spécifiques et les utilisateurs se voient attribuer ces rôles. Les utilisateurs obtiennent les permissions en fonction de leurs rôles.

**Caractéristiques**:

- **Rôles et Permissions** : Les permissions sont assignées à des rôles plutôt qu'à des utilisateurs individuels.
- **Gestion simplifiée** : La gestion des permissions est simplifiée en attribuant ou retirant des rôles aux utilisateurs.
- **Séparation des responsabilités** : Facilite la séparation des responsabilités et la conformité réglementaire.

**Exemple**:
Une entreprise où les rôles tels que "Administrateur", "Utilisateur", et "Visiteur" ont des permissions différentes. Les utilisateurs se voient attribuer des rôles en fonction de leurs responsabilités.

```
-- Exemple SQL de RBAC
CREATE ROLE Admin;
GRANT SELECT, INSERT, UPDATE, DELETE ON database TO Admin;
```

### Comparaison des Modèles

| Caractéristique | DAC | MAC | RBAC |
|---|---|---|---|
| **Contrôle des Permissions** | Propriétaire des objets | Administrateur central | Rôles définis par l'organisation |
| **Flexibilité** | Haute | Faible | Moyenne à haute |
| **Sécurité** | Moyenne | Très haute | Haute |
| **Gestion des Permissions** | Difficile à grande échelle | Centralisée et stricte | Simplifiée par les rôles |
| **Usage Typique** | Systèmes personnels, petites entreprises | Militaires, gouvernements | Entreprises, institutions |

### Conclusion

- **DAC** est flexible et convient aux environnements où les utilisateurs doivent contrôler directement l'accès à leurs propres ressources.
- **MAC** est utilisé dans des environnements où la sécurité est une priorité absolue et où des politiques de sécurité strictes doivent être appliquées sans exception.

- **RBAC** offre un bon équilibre entre sécurité et facilité de gestion, ce qui le rend idéal pour les organisations de taille moyenne à grande qui ont besoin de gérer les permissions de manière efficace.