

1 Exercice n° 1 : Questions de cours

1. Qu'est-ce qu'une politique de contrôle d'accès ?
2. Qu'est-ce qu'un modèle (de politique) de contrôle d'accès ?
3. Que signifient les sigles " ITSEC ", " DAC " et " MAC " ?
4. Expliquer les notions de contrôle d'accès discrétionnaire et contrôle d'accès obligatoire ;
5. La politique de contrôle d'accès aux fichiers sous Unix est-elle discrétionnaire ou obligatoire ? Argumenter.
6. Que signifient les termes " sujet " et " objet " dans une politique de contrôle d'accès ?
7. Qu'est-ce qu'une politique de contrôle d'accès " cohérente " ?

2 Exercice n° 2 : Matrice d'accès

Le sujet s_1 a un droit de lecture et d'exécution sur le fichier `toto.exe`. Le sujet s_2 peut exécuter `toto.exe`, lire et écrire le fichier `tata.txt`. Enfin s_1 à un droit de lecture sur le fichier `tata.txt`. Modéliser la matrice de contrôle d'accès qui représente ces autorisations.

3 Exercice n° 3 : Modélisation

Soit un système informatique dans lequel nous avons trois utilisateurs s_i , $i = 1, 2, 3$ et deux objets : une imprimante `imp` et un fichier `toto.txt`. On suppose que l'on a défini les autorisations suivantes :

- s_1 est le propriétaire de `toto.txt` ;
- `imp` est d'accès libre pour tout le monde ;
- `imp` ne peut imprimer un fichier que si la requête d'impression provient d'un sujet qui a le droit d'imprimer ce fichier ;
- s_2 peut lire et copier `toto.txt` ;
- s_3 peut imprimer tous les fichiers sur lesquels ils disposent d'un droit de lecture ;
- s_3 n'a aucun droit sur `toto.txt`.

1. Modéliser ces autorisations selon le modèle de Lampson (matrice d'accès) et selon le modèle de Take-Grant.
2. Mettre une évidence une faiblesse dans cette politique de contrôle d'accès.
3. Expliciter comment s_3 peut réussir à lire le contenu de `toto.txt` de deux façons différentes. Vous mettrez à jour la matrice d'accès et le graphe en fonction des changements des droits d'accès.

4 Exercice n° 4 : Ensembles des parties d'un ensemble fini

1. Donner l'ensemble des parties de l'ensemble $\{a, b, c\}$;

2. Quelle est la relation d'ordre naturelle sur un ensemble de parties ?
3. Cette relation est-elle totale ?
4. Donner l'infimum et le supremum de deux ensembles (pour cette relation d'ordre).
5. Soit un ensemble fini à n éléments. Combien cette ensemble contient-il de parties distinctes ? (Vous pourrez utiliser la formule du binôme de Newton $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ où l'on rappelle que $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ représente le nombre de choix de k objets parmi n .)

Correction de la dernière question :

Une partie de E peut contenir soit 0, soit 1, ..., soit n éléments. On définit F_k l'ensemble des parties de E qui ont k éléments ($0 \leq k \leq n$). Alors $|F_k| = \binom{n}{k}$. Donc $|\mathcal{P}(E)| = \sum_{k=0}^n |F_k| = \sum_{k=0}^n \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k} = (1 + 1)^n = 2^n$.

5 Exercice n^o 5 : Relations d'ordre (pour le modèle de Bell-La Padula)

1. La relation binaire sur $E = \{x, y, z\}$ suivante est-elle une relation d'ordre ? $y \preceq x$, $x \preceq z$, $x \preceq x$, $y \preceq y$ et $z \preceq z$.
2. Peut-on rajouter une information pour que la relation précédente devienne une relation d'ordre ?
3. Soit la relation binaire sur $\{w, x, y, z\}$ suivante : $w \leq w$, $x \leq x$, $y \leq y$, $z \leq z$, $w \leq y$, $w \leq z$, $x \leq y$, $x \leq z$.
 - (a) Est-ce une relation d'ordre ?
 - (b) Si oui, l'ordre est-il total ? (trouver deux éléments a, b tels que ni $a \preceq b$, ni $b \preceq a$ ne soient vrais.)
 - (c) Est-ce un treillis ?
4. On considère trois utilisateurs $U1, U2, U3$ possédant chacun un fichier F_1, F_2, F_3 (où 1 est le niveau d'habilitation ou de classification le plus élevé). On suppose que le propriétaire d'un fichier a les droits **W** ("lecture") et **R** ("écriture") sur ce fichier. Par ailleurs un utilisateur peut lire dans un fichier que si son niveau d'habilitation domine le niveau de classification du fichier. Un utilisateur peut écrire dans un fichier que s'il ne peut pas le lire (sauf s'il en est le propriétaire).
 - Donner la matrice d'autorisation dans ce cas particulier de modèle de Bell-La Padula.
 - Expliquer comment cette politique permet-elle d'éviter les fuites d'information d'un niveau de classification donné vers un niveau moins élevé.

Correction de la dernière question :

$U1$ a les droits **r, w** sur $F1$, **r** sur $F2$ et $F3$. $U2$ a les droits **r, w** sur $F2$, **w** sur $F1$ et **r** sur $F3$. $U3$ a les droits **r, w** sur $F3$, **w** sur $F1$ et $F2$.

$U1$ peut lire et écrire dans le fichier $F1$. Il peut lire $F2$ et $F3$, donc les informations ne peuvent aller que dans le sens de l'accroissement du niveau de classification. $U2$ peut lire et écrire dans $F2$. Il peut lire $F3$ et écrire dans $F1$. La seule possibilité qu'il ait c'est de copier une partie des contenus de $F2$ et $F3$ dans $F1$ ou $F2$ (accroissement du niveau de

classification : OK). Enfin $U3$ peut lire et écrire dans $F3$. Il peut écrire dans $F1$ et $F2$ et donc il ne peut que copier dans ces fichiers une partie du contenu de $F3$ (ok).