Jeudi, 11 Avril 2024

SECURITE DES BASES DE DONNEES

I. GENERALITES SUR LA SECURITE DES BASES DE DONNEES

1. Généralités

La sécurité des bases de données est un ensemble de moyen de contrôle et de mesure conçu pour protéger les bd contre les menaces accidentelle et intentionnelle afin de préserver la confidentialité, l'intégrité et la disponibilité d'une base de données. Elle doit pouvoir gérer et protéger les éléments suivants :

- Le SGBD
- Les données de la BD
- Toutes les applications associer
- Le serveur de BD (Physique ou virtuel)

Les bases de données sont des niches qui regorgent d'information précieuse car aujourd'hui celui qui détient l'information, détient le pouvoir ; elle constitue donc une cible de choix pour les pirates. Une entreprise dont les données ne sont pas sécurisées ou dont les données ont été voler peut avoir des conséquences sur les points suivants :

- Une compromission de la propriété intellectuelle : en cas de vole ou de divulgation de la propriété intellectuelle, il peut être difficile de maintenir ou de récupérer votre compétitivité.
- Continuité des opérations : certaines entreprises ne peuvent pas continuer à fonctionner tant que la violation n'est pas résolue
- Coût de la remédiation des violations, perte des chiffres d'affaire
- Atteinte a la réputation de la marque, perte de client

La sécurité des bds trouve dont tous sont sens car elle permet de protéger les données contre toutes accès non autoriser, toute corruption ou vole de données depuis la sécurité physique du matérielle jusqu'au contrôle des administrateurs et des accès en passant par la sécurité logiciel des applications.

2. Les 03 principaux piliers de la sécurité des bds

La sécurité des bd inclut 03 principales propriétés, à savoir :

- La confidentialité
- L'intégrité
- La disponibilité

➢ L'intégrité : consiste à s'assurer que les données ne sont ni modifiées, ni falsifier par des personnes non autoriser. Toutes fois, l'intégrité d'une bd consiste à empêche les parties de faire se qu'ils veulent tant que les conditions ne sont pas respectées tant que les contraintes d'intégrité ne sont pas respectées.

Menace :

- Introduction de données valide mais inexacte

- Introduction de données invalide
- Abus de privilège légitime
  - ➢ La disponibilité : consiste à s'assurer de l'accessibilité des données 24/24(h) et 7/7(jrs)

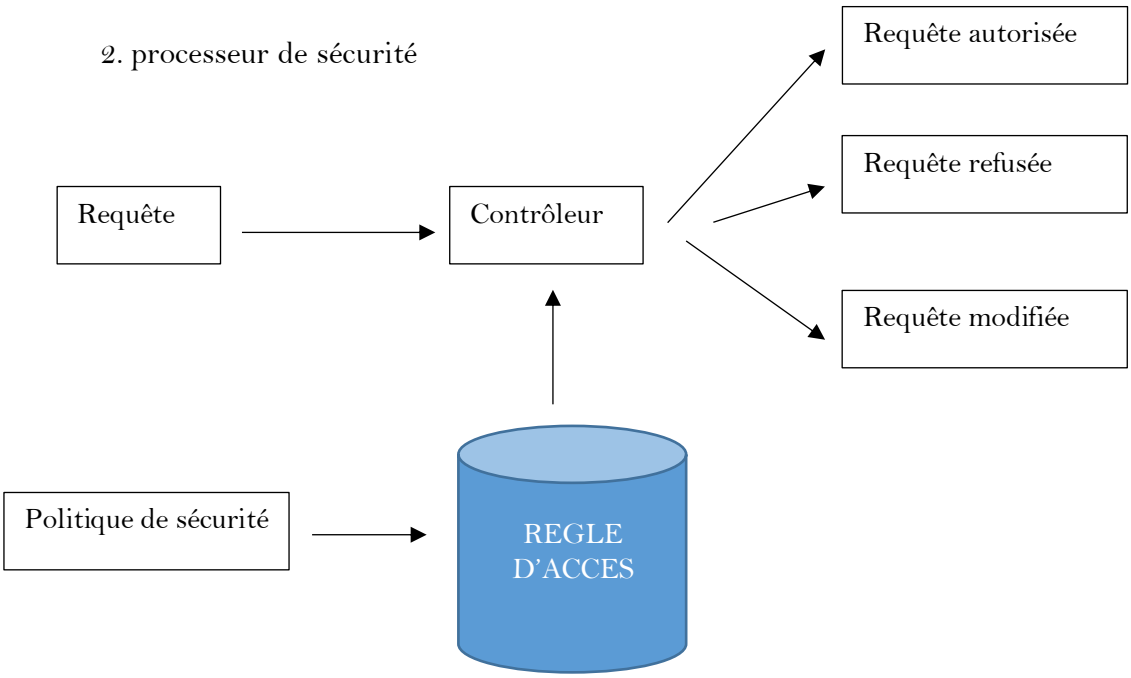
    Menaces :

    - Incident détruisant le support (crache)
    - Attaque par déni de service
  - ➢ La confidentialité : consiste à s'assurer que seules les personnes autoriser ont accès aux données

    Menaces :

    - L'abus de privilège légitime
    - La vente illégale des données utilisateurs

2. processeur de sécurité



Il s'agit ici de contrôler l'accès d'un programme ou d'un utilisateur aux données ou aux objets de la bd en vérifiant que les requetés adressés au système ne violent pas les réglé d'accès et selon le cas autorise, modifie ou refuse l'accès en fonction de la politique de sécurité de l'entreprise qui est traduite sous forme de règle d'accès.

3. Les attaques

Une attaque est une action destinée à porter atteinte à la sécurité d'un système d'information, elle représente la concrétisation d'une menace.

3.1. Les types d'attaque

On distingue deux types d'attaque, à savoir : les attaques frauduleuses et les attaques non frauduleuses

- Les attaques non frauduleuses : Coupure de courant, catastrophes naturelles, pannes logicielles et matérielles

- Les attaques frauduleuses : les attaques sur une BD peuvent exploiter les menaces suivant qui peuvent être à la fois internes et externe.

Lorsque les utilisateurs ou programmes ont des privilèges d'accès à une bd excédant les de leur fonction professionnelle, il peut abuser de ces privilèges à de fins malveillantes.

- Abus de privilège légitime : abus, les utilisateurs peuvent également abuser de leurs privilèges afin d'accéder à la BD à des fins non autorises.
- L'élévation de privilèges : technique qui consiste à un utilisateur disposant d'un accès restreint d'élargir le périmètre et l'étendue de ses autorisations voir à celui de l'administrateur. On distingue 02 catégories d'élévation de privilèges : l'élévation horizontale qui consiste à obtenir un accès privilégié a un compte utilisateur standard dotés de privilèges de niveau inférieur et une fois dans le système, l'attaquant étend son accès ; Elévation verticale qui consiste à obtenir un accès à des comptes dotés de privilèges et d'autorisations de niveau supérieur.
- Attaque par déni de service : dans une attaque par déni de service, le pirate inonde le serveur d'autant de demandes possibles de manière à ce que celui-ci ne puisse plus répondre aux demande légitimes des utilisateurs réels poussant ainsi le serveur à être instable ou bloqué.

4. L'injection SQL

Elle consiste à contre faire une instruction sdl de manière de la détourner de son objectif initial permettant ainsi à l'attaquant d'altérer, voler ou de détruire des données et dans le pire des cas d'accéder de manière totale à la BD.

a. Principe

Une injection SQL se produit lorsqu'un utilisateur malveillant communique une entrée qui modifie la requête SQL envoyée sur l'application web à la bd lui permettant alors d'exécuter d'autres requêtes non souhaitées. Pour ce fait, l'attaquant doit injecter du code en dehors des limites de L'entre utilisateur afin qu'il ne soit pas exécuté Comme une entrée standard.

Cas Pratique : contournement d'une authentification

L'injection sql fait référence aux attaques contre les bases de données relationnelles en revange, celles qui sont effectuées sur des Bd non relationnelle, sont des injections Nosql.

b. Les types de pirates

Sur une bd on peut avoir différents types d'attaquants :

- Les pirates administrateurs : personne qui se sert de leurs droits administrateurs ou qui le sont octroyés ces droits pour mieux espionner le système à des fonds malveillantes
- Les pirates utilisateurs : personnes reconnues par le système et voulant accéder a des données dont elles n'ont pas d'autorisations nécessaires

- Les pirates externes : personnes externes au système capable de s'infiltrer dans le seveur avec pour but L'altérer, voler ou supprimer des données.

c. Les risques encourus

- Les vols de données Conduit à la parte de la Confidentialité de l'entreprise et peut avoir un impact néfaste sur celle-ci.
- L'altération des données induit une perte de d'intégrités, les données ne sont plus dignes de confiance.
- La destruction des données remet sérieusement. En cause la continuité des activités de l'entreprise

d. Les types d'utilisateurs

On distingue trois principaux types d'user :

- Les administrateurs de la bd : qui assurent la gestion technique et nécessaire
- Les programmeurs d'application
- Les users finaux : ce sont ceux à qui l'admin à octroyer des droits

5. Les mesures de protection

Afin de garantie la sécurité d'un SGBD, plusieurs moyens peuvent être utilisées ;

5.1. Les Vues

Une vue est une table virtuelle qui contient le résultat d'une requête, elle ne stocke pas les données, elles conservent juste la requête permettant de les créer. Elle est utilisée en sécurité pour protéger les données donnant ainsi la possibilité de caché certains champs aux utilisateurs et de personnalisé l'affichage de certaine information suivant le type d'utilisateur.

Exemple :

```
CREATE VIEW daac as select etudiant.*,matiere.*, notes.note FROM matiere INNER JOIN notes on matiere.idmat = notes.idmat inner join etudiant on notes.matricule = etudiant.matricule;

CREATE VIEW secdaa as select etudiant.sexe, matiere.idmat, notes.note FROM notes INNER JOIN etudiant on notes.matricule = etudiant.matricule inner join matiere on matiere.idmat = notes.idmat ;

CREATE VIEW daacadjoint as select etudiant.matricule, etudiant.nom, etudiant.datnaiss, matiere.idmat, notes.note FROM etudiant INNER JOIN notes on etudiant.matricule = notes.matricule inner join matiere on notes.idmat = matiere.idmat;

GRANT ALL PRIVILEGES on daac to 'daac'@'localhost';
```

5.2. L'authentification

L'authentification est le processus ou l'acte de confirmation qu'un utilisateur qui tente de se connecter à une bd est bien celui qu'il prétend être. Avec une stratégie d'authentification et

d'autorisation bien réfléchis, les entreprises peuvent vérifier de manière efficace l'identité de chaque utilisateur et ceux a quoi ils ont accès ; ce qui est un facteur de renforcement de la sécurité de ses entreprises.

5.3 le contrôle d'accès

C'est un élément essentiel de la stratégie de sécurité et qui consiste à s'assurer qui est autorisé ou pas a accédé à certaine ressource de la bd. Un système de contrôle d'accès comprend :

- Des sujets : entité qui initie la demande d'accès
- Les objets : entité à laquelle le sujet souhaite accéder et qui contient des informations
- Les opérations (Read) déclencher par les sujets sur les objets
- Un ensemble de règle d'accès ou permission traduisant la politique de sécurité de l'entreprise

Modelé de contrôle d'accès

Il constitue la base de toutes politique en matiere de sécurité, il en existe plusieurs :

- Les modelés discrétionnaires encore appelé DAC (dictionnary access control)

Principe :

- Le créateur d'un objet est le propriétaire de cet objet
- Le propriétaire peut transmettre ou retirer à sa discrétion des autorisations sur ses objets a d'autre utilisateurs
- Le propriétaire peut transmettre a d'autre utilisateur le droit de transmettre ses autorisations
- Ce qui n'est pas autoriser est interdite

Exple de modelé discrétionnaire : modelé de lampson et HRU

La notion de matrice de contrôle d'accès est dédiée à la représentation des droits sou forme de matrice et a été introduit par lampson en 1971. La structure de se modèle est représenté sous forme d'un triplet (S, O, M) avec S : l'ensemble de sujets, O : ensemble des objet et M : la matrice de contrôle d'accès. Chaque cellule M (s, o) contient les droits d'accès que le sujet s possède sur l'objet o. les objets représente les colonnes et les sujets les lignes :

Sujets \ Objets	O1	O2
S1	-	R
S2	X	-
S3	-	W

Ce modèle a été améliorer pour donner naissance à HRU (Harrison, Ruzzo et Ullmann) en 1976 qui définis un quadruplet (S, O, R, M) ou S : ensemble des sujets, O : ensembles des objets, R : les modes d'accès et M : la matrice d'accès.

R comprend les accès suivants : Read, write, append, execute, own. La différence entre lampson et HRU réside dans le fait que HRU spécifie les commandes a attribué les droits ainsi que de créer et de supprimer les sujets et des objets.

NB : on peut ajouter un droit a) dans une matrice d'accès s'il existe une commande C qui ajoute le droit a dans une cellule de M(o)

Syntaxe :

Command NomCommande (X1, X2, ..., Xk)

If a1 in M (s, o1) and

If a2 in M (s2, o2) and

…

If am in M (sm, om)

Then op1 … opn

End

Il existe 6 opération primitive :

- Enter a into
- Delete a from
- Create subject s
- Create object o
- Delete object o

Exple :

- Creation d'une commande permettant d'attribuer le droit de lecture

Requête :

Command GrantRead (s1, s2, o1)

If own in M (s1, o1)

Then enter Read into M(s2,o1)

End

Formulation tabulaire :

Sujets\ Objets	S1	S2	O1
S1	Control		Own
S2		Control	Read

- Pour retirer le droit de lecture :

Command GrantRead (s1, s2, o1)

If own in M(s1,o1)

Then delete Read from M(s2,o1)

End

Sujets\ Objets	S1	S2	O1
S1	Control		Own

S2		Control	

- Dans l'entreprise lamda, le sujet s1 a le droit de lecture et d'exécution sur le fichier toto.exe ; le sujet s2 peut exécuter toto.exe, lire et écrire le fichier tata.txt et afin s1 a un droit de lecture sur le fichier tata.txt
  Taf : modéliser la matrice selon le modèle lampson et HRU
  Solution :
  - Lampson

  Nous avons : S= {s1,s2} : ensemble des sujets, O={toto.exe, tata.txt) : ensembles des objets

M(s1,toto.exe) = Read, execute

M(s1, tata.txt) = Read

M(S2, toto.exe)=execute

M(s2, tata.txt) = read, write

Sujets\objets	Toto.exe	Tata.txt
S1	R, X	R
S2	X	R, W

- HRU

Commande :

1)

Command readExecute (s1, toto.exe)

If R, X in M(s1, toto.exe)

Then enter R,X into M(s1,toto.exe)

End

2)

Command read (s1, tata.exe)
If R in M(s1, tata.exe)
Then enter R into M(s1,tata.exe)

End

3)

Command Execute (s2, toto.exe)
If X in M(s2, toto.exe)
Then enter X into M(s2,toto.exe)

End

4)

Command readWrite (s2, tata.txt)

If R, W in M(s2, tata.txt)

Then enter R,W into M(s2, tata.txt)

End

5.

Command LawRead (s1,s2, toto.exe)

If R* in M(s1, toto.exe)

Then enter R into M(s2, toto.exe)

End

6.

Command LawWrite (s1,s2, tata.txt)

If W* in M(s2, toto.exe)

Then enter W into M(s1, tata.txt)

End

Sujets\objet	S1	S2	Toto.exe	Tata.txt
S1	control		R,x	R,w
S2		control	X,r	R,w

Résultat : politique de sécurité de l'entreprise bafoué

- Devoir : soit 03 users s1, s2, s3 et deux objets : une imprimante imp. et un fichier toto.txt et soit les autorisations suivantes :
    - S1 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 de lecture sur ce fichier
    - S2 peut lire toto.txt
    - S3 peut imprimer tous les fichiers
    - S3 n'a aucun droit sur toto.txt

Taf : modéliser la matrice selon le modèle lampson et HRU

Solution : Nous avons : S= {s1, s2, s3} : ensemble des sujets, O= {toto.txt, imp) : ensembles des objets

Sujets (S) :

- S1 (Propriétaire de toto.txt)
- S2
- S3

Objets (O) :

- Imp (Imprimante)
- toto.txt

Opérations (A) :

- Lecture (R)
- Écriture (W)
- Execute(x)
- Impression (P)= rx

M (S1, toto.txt) = own

M (S2, toto.txt) = r

M (S3, toto.txt) = -

M (S1, imp) = x

M (S2, imp) = r

M (S3, imp) = r

M (S2, imp) = x

Voici la matrice de lampson :

Sujets \objets	Imp	toto.txt
S1	P	Own
S2	P	R
S3	X	-

Explications :

- S1 (Propriétaire de toto.txt) donc à tous les droits sur toto.txt.
- S2 a le droit de lecture (R) sur toto.txt.
- S3 a le droit d'impression (P) sur tous les fichiers, y compris toto.txt.

HRU

Les commandes :

Command GrantOption (s1, toto.txt)

If own in M (s1, toto.txt)

Then enter Read, Write into M (s1, toto.txt)

End

Command ReadOption (s2, toto.txt, imp)

If R in M (s2, toto.txt)

Then enter p into M (s2, toto.txt, imp)

End

Command GrantRead (s1, s2, s3, toto.txt)

If own in M (s1, toto.txt)

Then enter xw into M (s2, toto.txt)

And

Then enter rxw into M (s3, toto.txt)

End

Command GrantEx (s2, s3, toto.txt, imp)

If x in M (s1, toto.txt)

Then enter x into M (s3, imp)

End

Command GrantEx (s1, s3, imp)

If x* in M (s1, imp)

Then enter x into M (s3, imp)

End

Sujets\objets	S1	S2	S3	Imp	Toto.txt
S1	Control			P	Own
S2		Control		P	pw
S3			Control	P	Pw

Avantages et inconvénient des modèles discrétionnaires

Avantages :

- Facile à implémenter
- Offre une grande flexibilité
- Intégrer à la plus par des système Unix

Inconvénient :

- Ne reflété pas le flux d'information réel dans un système car les informations autoriser peuvent être copier d'un objet a un autre
- Risque d'explosion des ACL
- Modelé inadapté a un système comportant un nombre important d'utilisateur
- Est sujet a de nombreuse erreur lors de l'attribution des autorisations par le propriétaire de l'objet

- Aucune restriction ne s'applique à l'utilisation des informations lorsque l'utilisateur leurs a reçu

Modèles Obligatoires

Encore appelé MAC (Mandatory access control), ils ont été développer pour des systèmes d'information pour lesquelles la préservation du secret est primordiale (armé, gouvernement). L'accès aux objets est restrient en fonction de la sensibilité des infos contenu dans les objets et du niveau d'autorisation de l'user de disposer d'une telle sensibilité.

Principe : les objets se voir attribué une classification (top secret, secret, confidentielle, public etc…) tandis que les sujets possèdent une habilitation (niveau d'autorisation). Les règles qui régissent les autorisations d'accès sont basé sur une comparaison de l'habilitation de l'utilisateur et de la classification de l'objet.

Le contrôle d'accès obligatoire est utilisé lorsque la politique de sécurité de l'entreprise impose que les décisions de protection ne doivent pas être prise par le propriétaire des objets concernées.

Exple de modèle obligatoire :

a. Modelé de Bell et Lapadula

Modelé développer par David Bell et Leonard Lapadula en 1973 pour formaliser la politique de sécurité du département de la défense des USA. Ce modèle met l'accent sur la confidentialité des données :

- Interdit toutes fuites d'informations d'un objet avec un certain niveau de classification vers un objet de niveau de classification inférieur
- Interdit a tous sujet d'une certaine habilitation d'obtenir des infos d'un objet de classification supérieur a cette habilitation.

L'ensembles de niveau de sécurité est muni d'un nombre partiel supérieur ou égale (>=) :

On a : **Top secret >= secret >=confidentiel >=public >= NC**

Propriétés de sécurité : un état est sécuritaire s'il vérifie les propriétés suivantes :

- **La simple propriété de sécurité ou No Read Up** : un sujet ne peut accéder à un objet que si son niveau de sécurité est >= a celui de l'objet

Explication : un sujet qui a l'habilitation confidentiel par exemple n'a pas le droit d'accédé en lecture a un objet qui a la classification top secret parce que le niveau de sécurité confidentiel est inferieur a celui de top secret par contre un sujet qui a l'habilitation top secret a le droit d'accédé en lecture a un objet qui a la classification confidentielle parce que le niveau de sécurité confidentiel est inférieur à celui de top secret (je ne peux pas lire en montant). La satisfaction de cette propriété assure qu'un sujet n'accèdera jamais à une info classée à un niveau plus haut que lui.

- **La propriété * ou No Write Down** : un sujet ne peut accéder en écriture a un objet ssi le niveau de sécurité du sujet est <= au niveau de classification de l'objet.

Explication : un sujet qui a l'habilitation confidentielle a le droit d'accédé en écriture a un objet qui a la classification top secret ou secret parce que sont niveau de sécurité confidentiel est inférieur au niv de sécurité top secret par contre un sujet qui a l'habilitation top secret n'a pas le droit d'accédé en écriture a un objet qui a le niv confidentiel.

Exple : soit les éléments suivants : S = {bob, Sonia}, O = {fichier personnels, fichier du courriel, fichier log, fichier des coordonnées}, L = {top secret, secret, confidentiel, NC} avec **top secret** le haut du système et **NC** le bas du système.

Niveau de sécurités	Sujets	Objets
Top secret	Bob	Fichier personnels
Secret		Fichier du courriel
Confidentiel		Fichier log
Non Classé	Sonia	Fichier des coordonnées

Taf : Ecrive les règles qui découle de ce tableau en fonction de modèle Bell et Lapadula puis représenter la matrice de contrôle d'accès du modèle de Lampson.

Solution :
Suivant la propriété no Read up et no write down nous avons :

- Bob a le droit de lecture et écriture sur le fichier personnel parce que son niveau d'habilitation est égal au niveau de classification top secret.
- Bob a le droit de lecture sur le fichier courriel parce que son niveau d'habilitation est supérieur au niveau de classification secret.
- Bob a le droit de lecture sur le fichier log parce que son niveau d'habilitation est supérieur au niveau de classification confidentiel.
- Sonia peut lire et écrire sur fichier de coordonnées parce que sont niveau d'habilitation est égale au niveau de classification
- Sonia a le droit d'écriture sur tous le reste des fichiers
- Bob n'a pas le droit d'écriture sur tout le reste des fichiers …
- Sonia n'a pas le droit de lecture sur tous le reste des fichiers

Modèle de Lampson :

M (bob, Fp) =rw

M (bob, Fc) =r

M (bob, Flog) =r

M (bob, Fcood) =r

M (Sonia, Fp) =w

M (Sonia, Fc) =w

M (Sonia, Flog) =w

M (Sonia, Fcood) =wr

Sujets\Objets	Fp	FC	Flog	FCoord
Bob	Rw	R	R	R
Sonia	W	W	W	Wr

b. Le modèle de Biba

C'est un modèle développer par Kennet Biba en 1977 qui formalise la sécurité multi niveau et met l'accent sur l'intégrité des données. Tous comme le modèle de Bell et Lapadula, le modèle de Biba est défini par deux propriété : la simple et étoile (*).

- **Propriété simple ou No Read Down** : cette propriété interdit a un sujet d'accédé en lecture a un objet qui a une classification moins élevée que l'habilitation de ce sujet.
  Explication : un sujet qui a l'habilitation confidentielle par exemple a le droit d'accède en lecture a un objet qui a la classification top secret parce que son niveau de sécurité est inferieur au niveau de sécurité top secret ; par contre un sujet qui a l'habilitation top secret n'a pas le droit d'accédé en lecture a un objet qui a la classification confidentielle.
- **La propriété * ou No Write Up** : cette propriété interdit a un sujet d'accédé en écriture a un objet qui a une classification plus élevée que son habilitation.
  Explication : un sujet qui a l'habilitation confidentielle par exemple n'a pas le droit d'accédé en écriture a un objet qui a la classification top secret parce que le niveau de sécurité confidentielle est inferieur au niveau de sécurité top secret ; par contre un sujet qui a l'habilitation top secret a le droit d'accédé en écriture a un objet qui a la classification confidentielle parce que le niveau de sécurité top secret est supérieur au niveau de sécurité confidentielle.

D'après l'exemple précèdent (Bell et Lapadula) on a :

Solution : les règles suivantes :

- Bob a le droit de lecture et écriture sur le fichier personnels parce que son niveau d'habilitation est égal au niveau de classification.
- Bob a le droit d'écriture sur tous les autres fichiers parce que son niveau d'habilitation est égal au niveau de classification haut
- Bob n'a pas le droit de lecture sur fichiers de courriel parce que son niveau d'habilitation…
- Sonia peut lire et écrire sur fichier de coordonnées parce que son niveau d'habilitation est égal au niveau de classification
- Sonia a le droit de lecture sur tout le reste des fichiers …
- Bob n'a pas le droit de lecture sur tout le reste des fichiers …
- Sonia n'a pas le droit d'écriture sur tout le reste des fichiers…

Modèle de Lampson :

M (bob, Fp) =rw

M (bob, Fc) =w

M (bob, Flog) =w

M (bob, Fcood) =w

M (Sonia, Fp) =r

M (Sonia, Fc) =r

M (Sonia, Flog) =r

M (Sonia, Fcood) =wr

Sujets\Objets	Fp	FC	Flog	FCoord
Bob	Rw	W	W	W
Sonia	R	R	R	Wr

Devoir : Présenter les avantages et inconvénients du MAC

Avantages :

- Ils sont bien adaptés aux applications où la protection du secret et de l'intégrité est primordiale.
- **Cohérence** : garantissent que toutes les bases de données sont sécurisées de manière cohérente, car ils imposent des normes et des pratiques de sécurité uniformes. Cela réduit les risques de vulnérabilités et d'erreurs humaines.
- **Conformité réglementaire** : aident les organisations à se conformer aux réglementations en matière de sécurité des données, telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne. Ils fournissent des directives claires et obligatoires qui aident à éviter les sanctions légales et les amendes.
- **Réduction des risques** : En imposant des mesures de sécurité spécifiques, les modèles obligatoires réduisent les risques de violations de données, de fuites d'informations sensibles et d'accès non autorisé aux bases de données. Cela contribue à protéger la réputation de l'entreprise et la confidentialité des données des utilisateurs.
- **Meilleures pratiques** : Les modèles obligatoires encouragent l'adoption de meilleures pratiques de sécurité des bases de données. Ils peuvent inclure des directives sur la gestion des mots de passe, le chiffrement des données, la définition des autorisations d'accès et d'autres mesures de sécurité essentielles

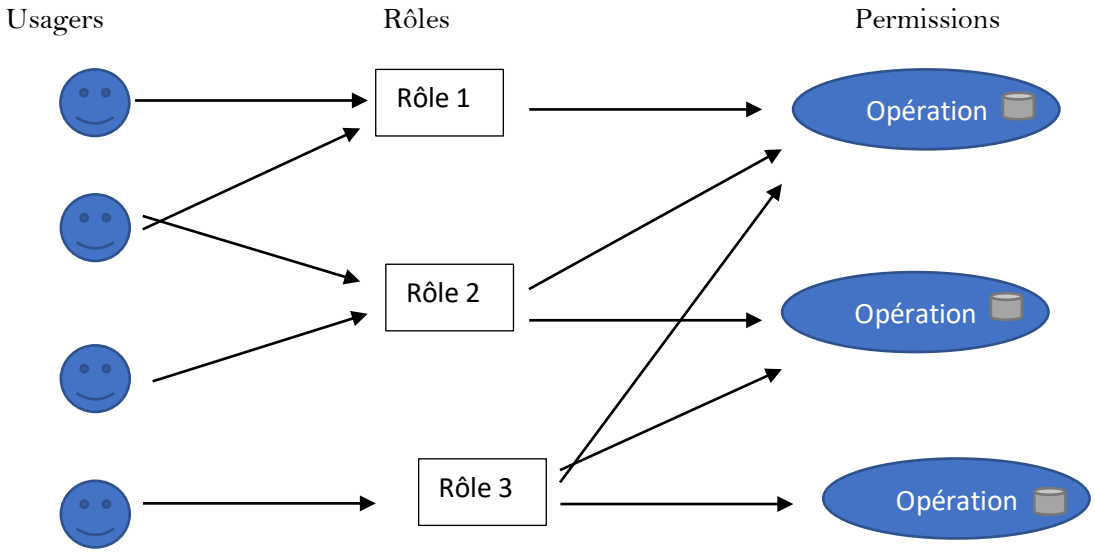
Inconvénients :

- Mais ils sont trop rigides et centralisés : La confidentialité est assurée au détriment de la disponibilité.
- **Complexité** : ils peuvent être complexes à mettre en œuvre, en particulier dans les grandes organisations disposant de plusieurs bases de données et de multiples systèmes. La mise en place de mesures de sécurité uniformes peut nécessiter des efforts considérables en termes de coordination et de formation.
- **Coût** : L'adoption de modèles obligatoires de sécurité des bases de données peut entraîner des coûts supplémentaires. Cela peut inclure les investissements nécessaires pour mettre à niveau les infrastructures, former le personnel et mettre en place des solutions de sécurité supplémentaires.
- **Flexibilité limitée** : ils peuvent parfois limiter la flexibilité des entreprises en matière d'innovation et de personnalisation des solutions de sécurité. Certaines organisations pourraient estimer que les modèles standardisés ne répondent pas pleinement à leurs besoins spécifiques.

Les modèles à base de rôle

Encore appelé RBAC (Role Base Access Control) peut être considérer comme une approche alternative au contrôle d'accès obligatoire et discrétionnaire. Dans ce modèle, les permissions sont affectées à des rôles au lieu d'être affecter directement aux sujets. La motivation principale de ce modèle est de facilité d'administration des privilèges pour un grand

nombre d'utilisateur accédant à des ressources spécifiques. Le but est de regroupe les utilisateurs dans des rôles reflétant la structure de l'entreprise puis de distribué des permissions a ces rôles au lieu de le répéter pour chaque individu.



Explication : plusieurs sujets peuvent être attribué à plusieurs rôles ou aucun ; plusieurs rôles un sujet a une permission P ssi celui-ci est attribué à un rôle R qui détient cette permission.

Le RBAC est considéré comme un système idéal pour les entreprises dont la fréquence du changement du personnelle est élevé.

TP : à l'iai-cameroun, la direction des affaires académique est chargé de la gestion des notes des étudiants et a à se tête une directrice qui possédé les pleins droits sur les différentes entités, les responsables de filière sont chargé de consulter, insérer et modifier les notes et ont également une vue totale sur les infos des étudiants ainsi que des matiere dispensé ; le directeur adjoint quant a lui est chargé de la gestion complète des étudiants et a une vue globale sur les notes et matières dispensées. Les secrétaires quant à elles ne peuvent qu'insérer, consulter et modifier les infos des étudiants.

Soient les utilisateurs suivants :

- Anga directrice des affaires académique
- Salabessies direction adjoint
- Agbor responsables des filières software
- Belinga responsable des filière GL
- Salabessies responsables des filière Réseau
- Angouda secrétaire de la directrice
- Pani, EOUNOU et Bell secrétaire des responsables des filières

TAF : représenter le modèle RMAC de cette direction

Les rôles	Les utilisateurs
DAA	ANGA
Responsable de filière	SALABESSEES
DAA adjoint	AGBOR
Secrétariat	BELINGA
	PANI

	ANGOUNDA
	EWUNU
	BELL

Permissions :

- DAAC : Tous droits sur les étudiants notes et matière
- RF : insert, update, select sur les note et Select sur etudiant et matiere
- DAACAd : tous droit sur les étudiants et select sur note et matiere
- Sec : insert, select et update sur les étudiants

En console :

Create user username identified by 'password' ;

Create role nomrole ;

GRANT all PRIVILEGES on testcoursécurité. * to DAAC ;

- Activation des rôles :

  Set role nomrole ;

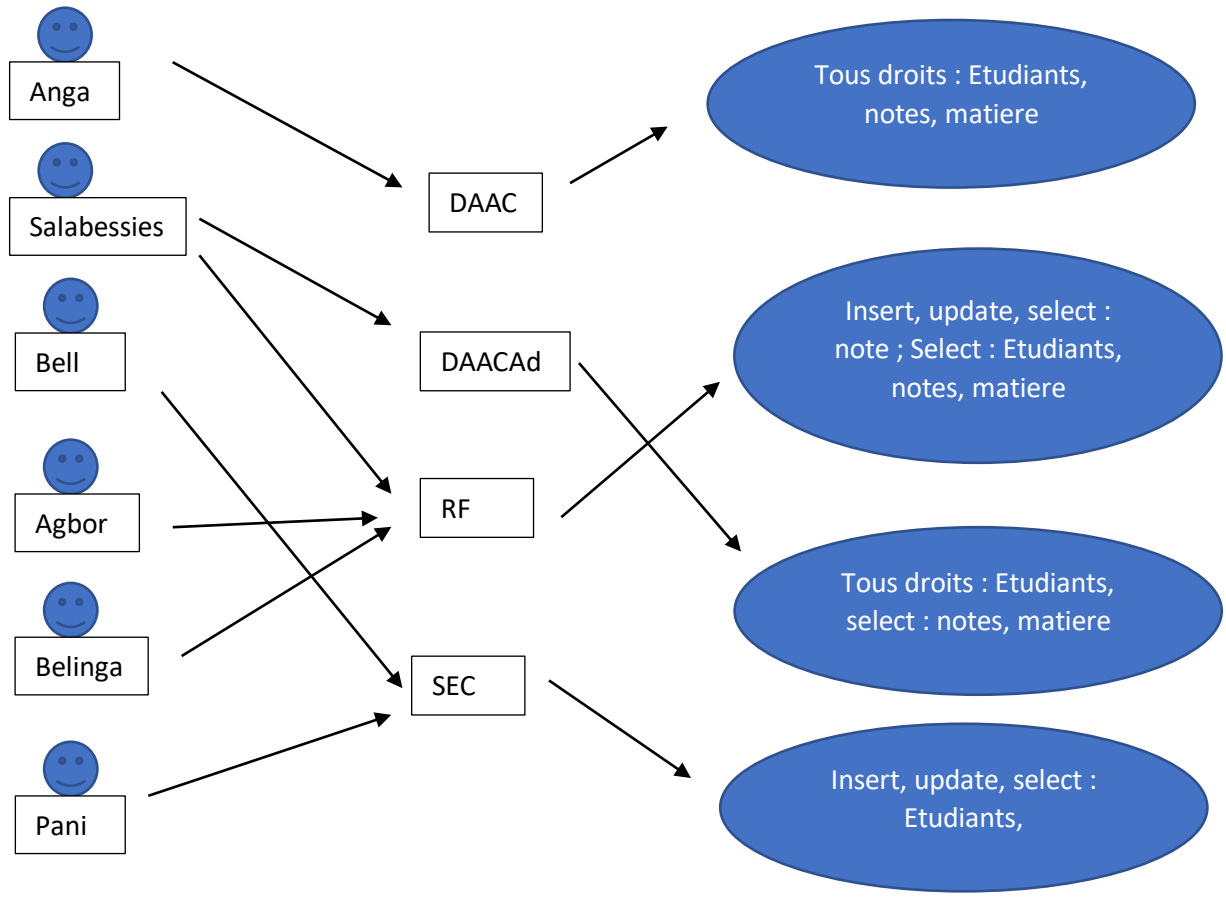
- Affectation d'un rôle a un utilisateur :
  Grant nomrole to username ;
- Pour supprimer un utilisateur d'un rôle :

  Revoke nomrole to username ;

- Afficher les roles auquel un utilisateur est lié :

  Show Grant for Anga using Daac ;

Modèle RBAC :



Bien.

4.6.2. Politique de gestion des privilèges

Règle 1 : attribution du moindre privilège : les users ne doivent avoir que le minimum de droit strictement nécessaire a l'accomplissent de leur tâche. Les privilèges peuvent évoluer au cours du temps, mais a un moment donné seuls les droits indispensables doivent être fournis à un utilisateur.

Règle 2 : contrôle de la population : le personnel d'une entreprise bouge, il Ya des départs, arriver… les privilèges doivent donc être synchrone avec la totalité de la population.

Règle 3 : contrôle physique des connexions : la connexion d'un user à une bd peut être réaliser m'importe ou grâce a internet, il est donc nécessaire de restreindre des connexions a des hautes spécifiques.

Règle 4 : limitation des ressources utilisées ;

Règle 5 : journaliser les comportements suspects. Certains SGBD permettent de conserver dans le fichier log des requetés non conforme au privilèges accordé à un utilisateur.

II. Les 8 états de la sécurité des bases de données

1. La découverte
2. Evaluation des vulnérabilités et la configuration
3. Renforcement(recommandation)
4. Audit des modifications
5. Surveillance des activités de la bases de données
6. Audit
7. Authentification, contrôle d'accès et gestion des droits
8. Chiffrements