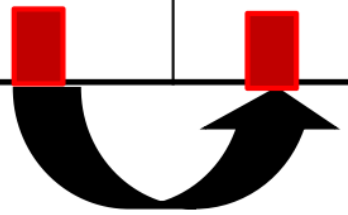
Limites du modèle DAC

	Dossier médical	Ordonnance
Médecin	RW	RW
Patient (Attaquant)	-	R
Application piégée	RW	RW

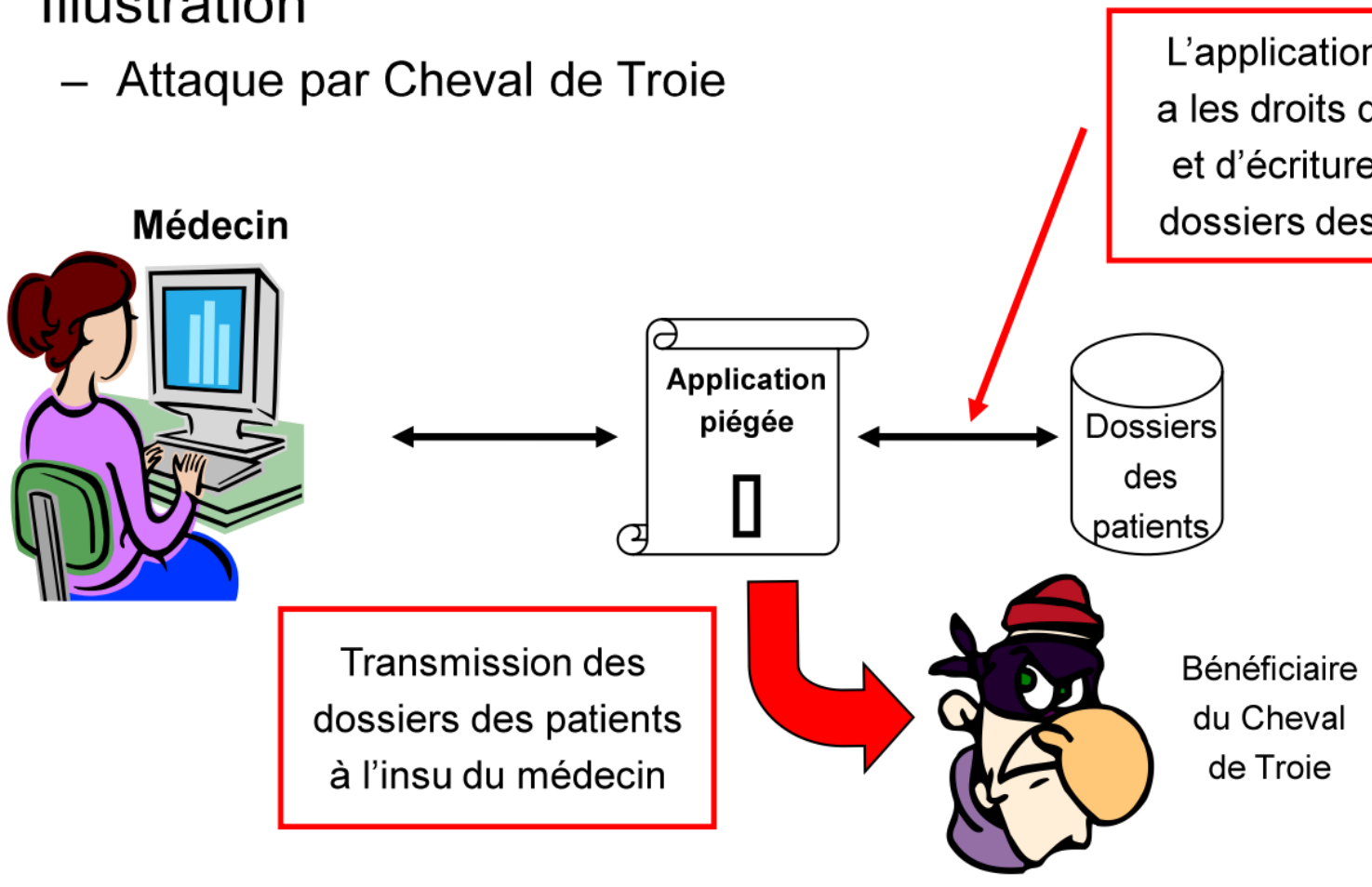


Transfert illégal non contrôlé par DAC

Application s'exécutant pour le compte du médecin (hérite des droits du médecin dans DAC)

Limites du modèle DAC

- Illustration
  - Attaque par Cheval de Troie



MAC

- MAC = Mandatory Access Control
  - Contrôle d'accès obligatoire
- MAC ajoute des étiquettes à chaque sujet et objet
- Une politique d'accès contient les règles d'accès permises pour chaque sujet et objet
- Politique par défaut
  - REFUSÉ (« Deny ») : l'accès n'est pas permis, à moins qu'il y ait une règle indiquant le contraire dans la politique d'accès
- Les règles et étiquettes peuvent seulement être changées par un administrateur avec un logiciel de confiance (« trusted »)

Politique de sécurité multiniveau

- Exemple classique de contrôle d'accès MAC
- Etiquette = niveau de sécurité
- Exemple

Public ≤ Confidentiel ≤ Secret

Politique de sécurité multiniveau

- Les utilisateurs reçoivent un niveau d'habilitation
  - Les utilisateurs s'engagent à ne pas diffuser n'importe comment les informations qu'ils détiennent
- Les informations reçoivent un niveau de classification
  - Mesure la confidentialité de l'information

Conditions de sécurité (Modèle de Bell & LaPadula)

- No Read Up
  - Un sujet s peut lire un objet o si :
    - niveau_classification(o) ≤ niveau_habilitation(s)
- No Write Down
  - Un sujet s peut modifier un objet o si :
    - niveau_habilitation(s) ≤ niveau_classification(o)

Conditions de sécurité (suite)

- Objectif du « No write down »
  - Soit un programme s'exécutant au niveau « Secret »
  - Ce programme peut lire des données classées « Secret »
  - Mais le « No write down » empêche un éventuel piège contenu dans ce programme de transmettre les données lues vers un utilisateur qui ne serait pas habilité au niveau « Secret »

Conditions de sécurité (suite)

Utilisateur habilité
« Secret »
(Médecin)

Application piégée

Lecture / Ecriture

Informations secrètes

Ecriture

No
« Write Down »

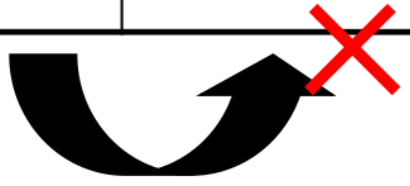
Fichier classé « Public »

Lecture

Utilisateur habilité « Public »

Conditions de sécurité (suite)

	Dossier médical (classé S)	Ordonnance (classé P)
Médecin (habilité S)	RW	RW
Attaquant (habilité P)	-	R
Application piégée (niveau S)	RW	R W



Transfert illégal bloqué par Bell et LaPadula

Conditions de sécurité (suite)

	Dossier médical (classé S)	Ordonnance (classé P)
Médecin (habilité S)	RW	RW
Attaquant (habilité P)	-	R
Application piégée (niveau courant S)	RW	~~RW~~
Application piégée (niveau courant P)	~~RW~~	RW

Intérêt du niveau courant : le médecin doit travailler au niveau P pour pouvoir écrire l'ordonnance

MAC

- Conditions de Bell & LaPadula trop rigides

- Aujourd'hui utilisation d'un autre modèle MAC
  - DTE (Domain Type Enforcement)
  - Implanté dans SELinux (Security Enhanced Linux)

Pourquoi RBAC ?

- DAC est de gestion difficile car chaque usager est un cas individuel
  - Considérez des compagnies de milliers d'employés

- DAC suppose que les usagers sont propriétaires des ressources et peuvent transférer les droits sur elles,
  - Tandis que normalement c'est l'organisation qui est propriétaire des ressources, et veut en retenir le contrôle

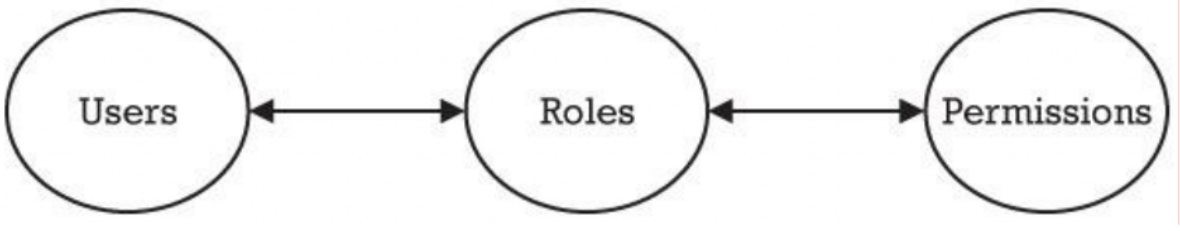
RBAC

- RBAC = Role Based Access Control

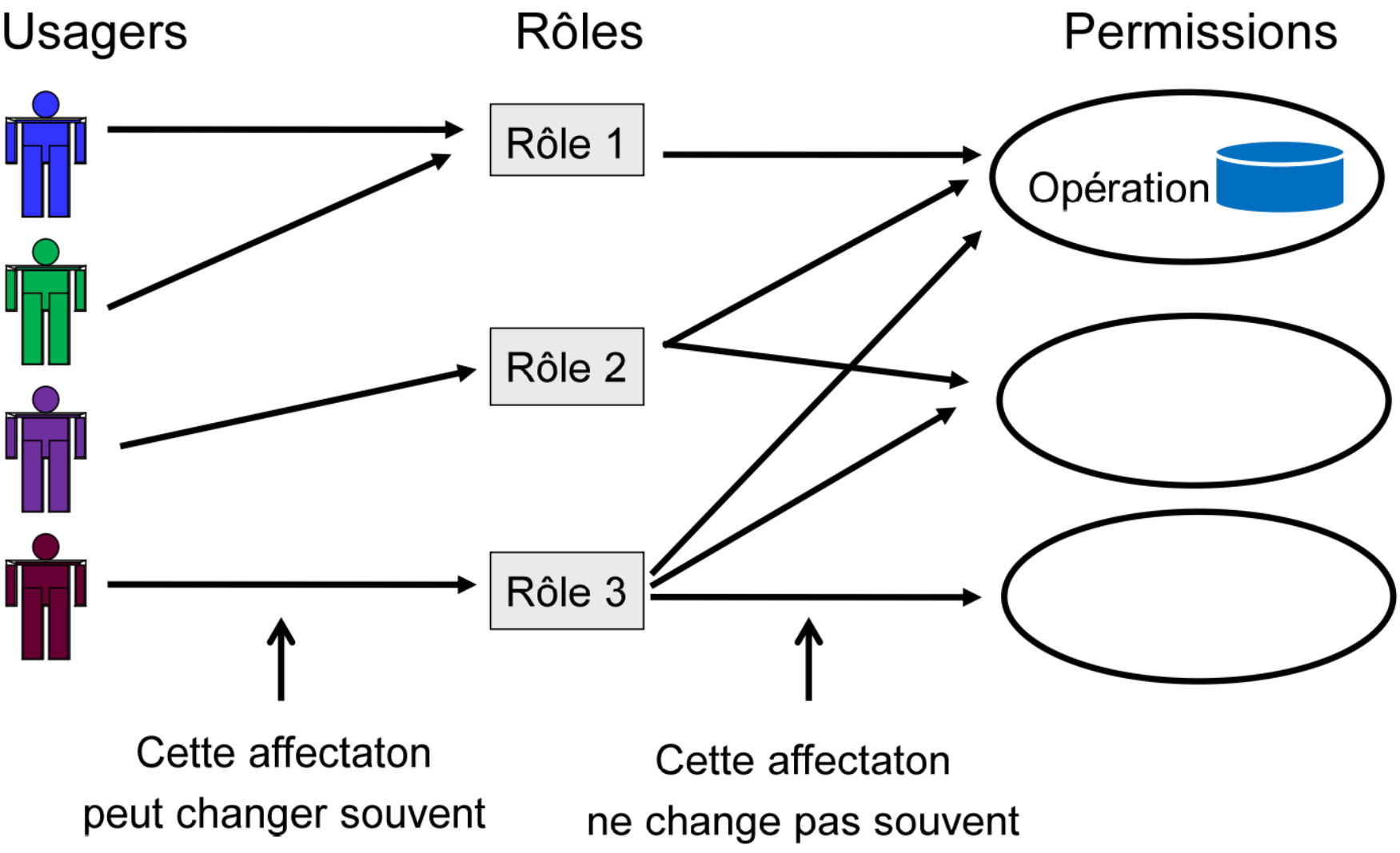
- RBAC est basé sur deux points
  - Le fait que dans les organisations les employés sont affectés à des rôles
    - Comptable, programmeur, docteur, infirmière, technicien …
    - Les rôles sont organisés en **hiérarchies**
  - Le fait que chaque employé, pour exécuter son rôle, a besoin de certaines permissions

RBAC

- RBAC s'appuie sur la notion organisationnelle de rôle pour associer des permissions de sécurité aux différents rôles
- Le rôle devient un mécanisme pour associer des permissions aux usagers



RBAC

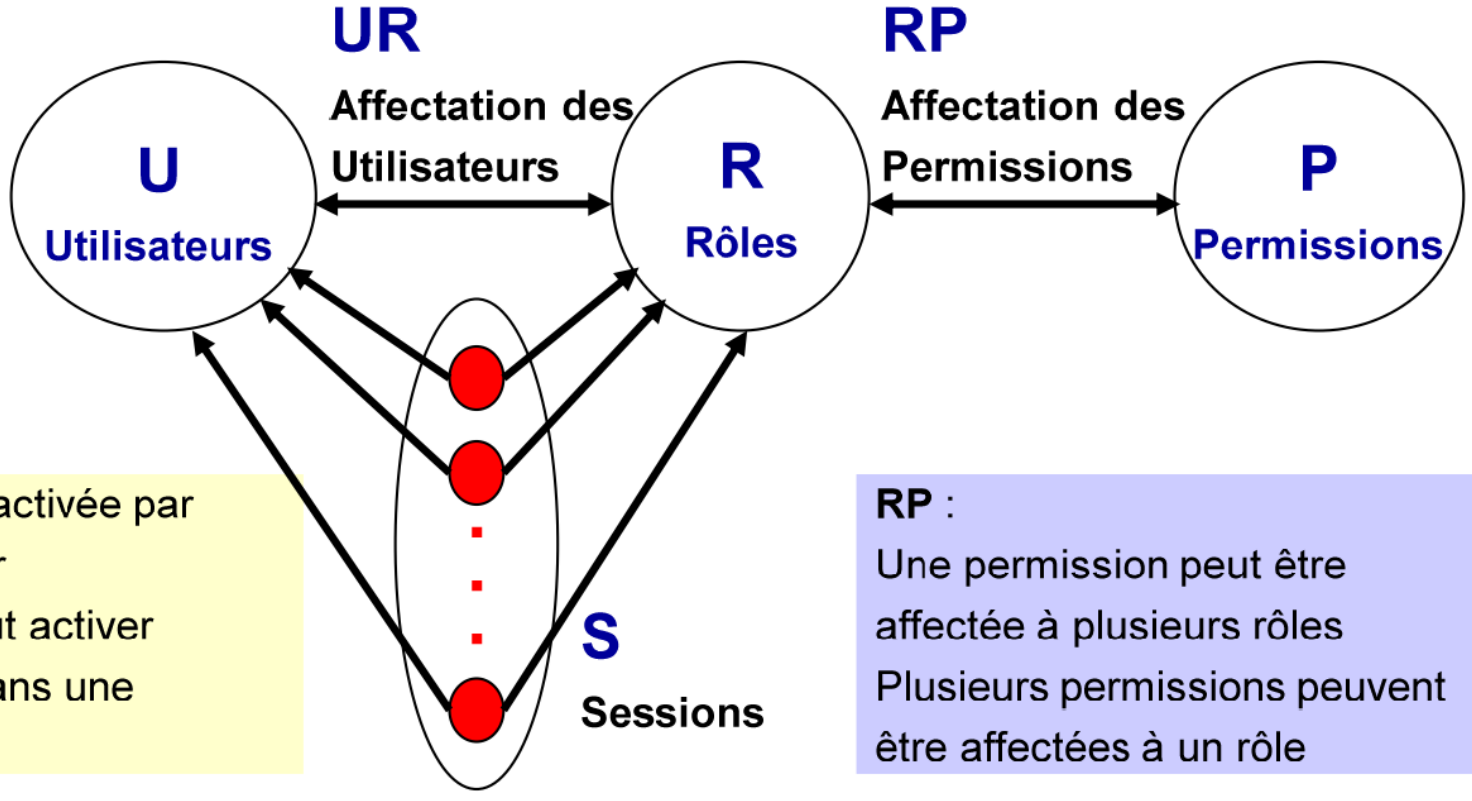

Usagers
Rôles
Permissions
Rôle 1
Rôle 2
Rôle 3
Opération
Cette affectaton
peut changer souvent
Cette affectaton
ne change pas souvent

RBAC
Concept de session

- Pour utiliser ses rôles, un usager doit activer des sessions
- Une session est un processus qui agit pour un usager
  - En changeant de session, un usager peut activer de nouveaux rôle(s)
  - P.ex. un employé de banque Paul peut activer un rôle quand il est aux prêts et un autre rôle quand il est aux investissements
- Pour accéder à une session, un sujet doit s'authentifier
- Un sujet peut se trouver dans plusieurs sessions simultanément

RBAC

UR :
Un rôle peut être
affecté à plusieurs utilisateurs
Plusieurs rôles peuvent
être affectés à un utilisateur

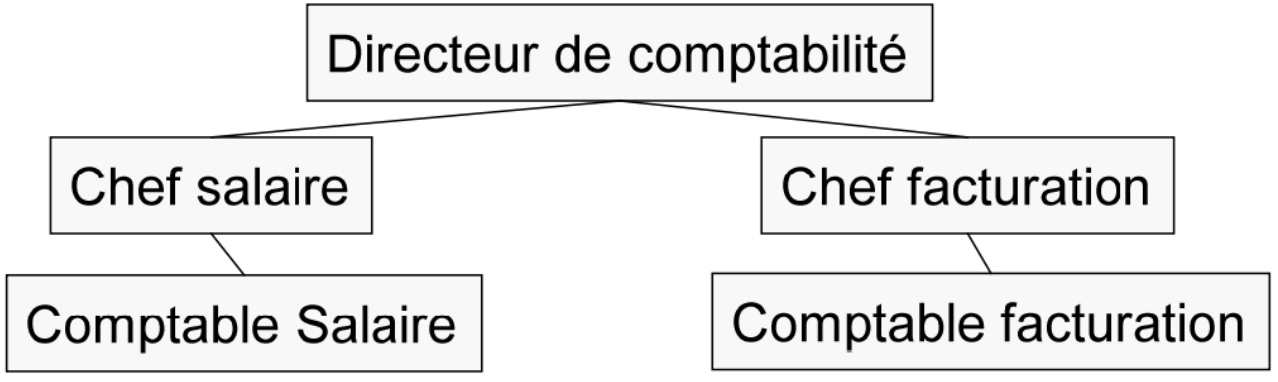


Une session est activée par
un seul utilisateur
Un utilisateur peut activer
plusieurs rôles dans une
session

RP :
Une permission peut être
affectée à plusieurs rôles
Plusieurs permissions peuvent
être affectées à un rôle

RBAC Hiérarchique

- On peut introduire une hiérarchie de rôles
- Propriété de cette hiérarchie
  - Héritage des permissions



  - Si Comptable Salaire a une permission, alors le Chef Salaire et le Directeur de Comptabilité l'ont aussi

RBAC avec contraintes

- Les contraintes sont un élément extrêmement important de RBAC
  - Les contraintes servent à empêcher certaines situations indésirables
- Exemple : contrainte de cardinalité
  - Il ne doit y avoir qu'un seul utilisateur affecté au rôle de directeur

RBAC avec contraintes

- Contraintes de « séparation des pouvoirs »
  - En anglais : « Separation of duty » (SOD)
  - Ce sont les contraintes les plus importantes
  - Exemple : Celui qui approuve un chèque (rôle R1) ne peut pas être celui qui le signe (rôle R2)
  - Dans RBAC, cela se traduit par une contrainte qui rend impossible qu'un utilisateur soit affecté à R1 et R2

- SOD statique (SSOD) ou dynamique (DSOD)
  - SSOD : la séparation s'applique en toute situation
  - DSOD : la séparation s'applique uniquement dans une même session

AGLP

- AGLP
  - Access – Global – Local – Permissions
  - Implémentation de RBAC sous Windows
  - Repose sur les Active Directory(AD)
- Éléments
  - Groupe « Globaux »
    - regroupement des utilisateurs, typiquement selon leur rôles
    - généralement définis sur des serveurs de domaine globaux (d'où le nom)
  - Groupes « Locaux »
    - auxquels sont attribués des Permissions sur des ressources
    - généralement définis et résidants sur les serveurs où ces ressources se trouvent (d'où le nom)
    - les membres sont exclusivement des groupes globaux