Organisation des droits d'accès aux systèmes d'information

ÉCOLE THÉMATIQUE BDA
Journée : protéger les données

Romuald THION

INRIA GRENOBLE – RHÔNE-ALPES
Équipe LICIT
http://licit.inrialpes.fr/~thion/

Jeudi 20 mai 2010

Plan

Objectifs de l'intervention

. . . security objectives shall be addressed by a combination of system security enforcing functions, and also by physical, personnel, or procedural means associated with the system.

Protéger les données

- définir les droits,
- vérifier les accès *a priori*,
- un des moyens de protection.

Protection logique

Distinction

- préalable : authentification
- ensuite : contrôle d'accès

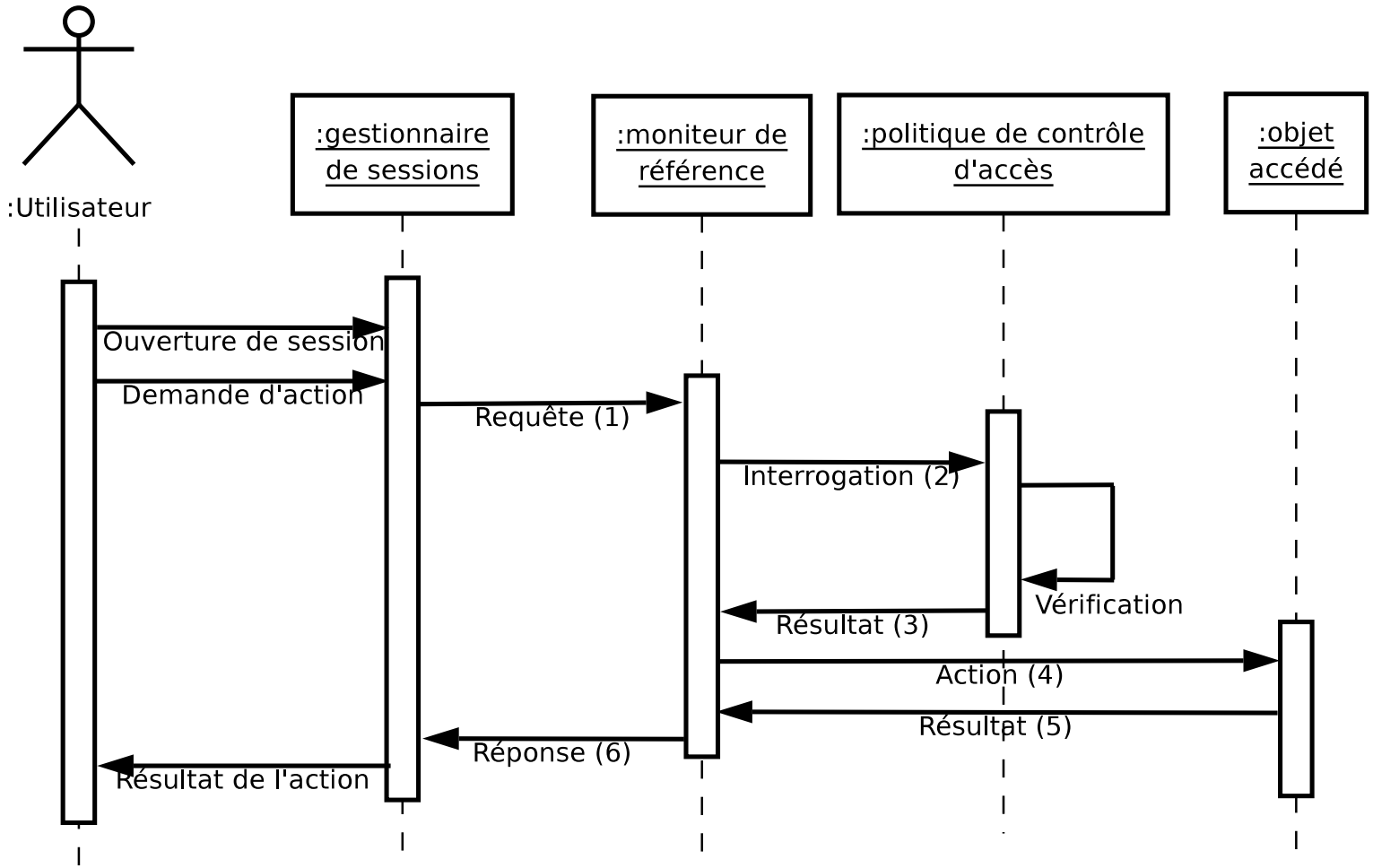
Contrôle d'accès : définition

Le contrôle d'accès est un mécanisme grâce auquel un système autorise ou interdit les actions demandées par des sujets sur des objets .

Contrôle d'accès

- un moyen mis en œuvre *a priori*,
- pour s'assurer de la légitimité des accès,
- selon une politique déterminée.

Le moniteur


:Utilisateur
:gestionnaire de sessions
:moniteur de référence
:politique de contrôle d'accès
:objet accédé
Ouverture de session
Demande d'action
Requête (1)
Interrogation (2)
Vérification
Résultat (3)
Action (4)
Résultat (5)
Réponse (6)
Résultat de l'action

L'organisation des droits

Principes généraux

- classification selon sensibilité,
- moindre privilège,
- séparation des tâches,
- conflits d'intérêts.

Survol du domaine

- modèles classiques,
- modèles à rôles,
- nouvelles générations.

Exemple académique

Un professeur gère l'accès à ses cours :

- donne des accès nominativement (identifiants),
- donne des accès à des agrégats de sujets (groupes).

Le professeur désire certaines propriétés :

- tous ses étudiants doivent avoir accès en lecture aux cours (disponibilité),
- aucun étudiant ne peut modifier les ressources (intégrité),
- les étudiants qui ne suivent pas son cours ne peuvent pas accéder aux ressources (confidentialité)

Modèles discrétionnaires

Trusted Computer System Evaluation Criteria, DoD, *1985* :

> *. . . a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).*

Particularités

- modèles historiques,
- décentralisés,
- difficiles à contrôler.

Matrice de contrôle d'accès

Matrice jouet

	Fichier1	Fichier2	Fichier3	Fichier4
Alice	rw	r	r	
Bob	r	rw	r	rwx
Charly	r	r	rw	rwx
Denise			r	r

Gestion des droits

Deux lectures

- permissions en lignes : *Capabilities List* (CL),
- permissions en colonnes : *Access Control List* (ACL).

Matrice sous forme de listes

```
GRANT r
  ON : Fichier1, Fichier2,
       Fichier3
  TO : Alice, Bob
GRANT w
  ON : Fichier1
  TO : Alice
  ON : Fichier2
  TO : Bob.
```

```
SUBJECT Alice
  IS GRANTED r
  ON : Fichier1, Fichier2,
       Fichier3
  IS GRANTED w
  ON : Fichier1.
SUBJECT Bob
  IS GRANTED r
  ON : Fichier1, Fichier2,
       Fichier3
  IS GRANTED w
  ON : Fichier2.
```

Modèles mandataires

Contrôle d'accès mandataire – MAC

Le contrôle d'accès mandataire est exprimé en termes de niveaux de sécurité associés aux sujets et aux objets et à partir desquels sont dérivés les actions autorisées.

Particularités

- Niveau d'indirection intermédiaire,
- Fortement centralisés,
- Rigides mais contrôlables.

Classification française

Classification	Description
Très Secret-Défense	Le niveau *Très Secret-Défense* est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense.
Secret-Défense	Le niveau *Secret-Défense* est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale.
Confidentiel-Défense	Le niveau *Confidentiel-Défense* est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié au niveau *Très Secret-Défense* ou *Secret-Défense*.

Dérivations des autorisations

Deux règles

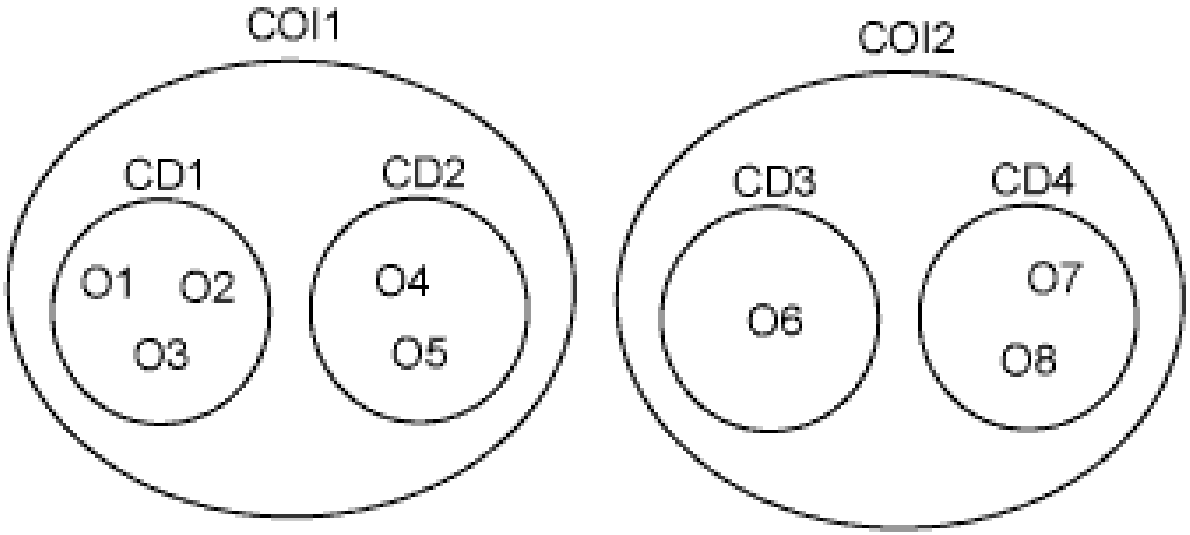
Propriété	Description
No read up[a]	Un sujet accrédité d'un niveau donné ne peut pas accéder en *lecture* à des objets d'un niveau plus élevé
No write down[b]	Un sujet accrédité d'un niveau donné ne peut pas accéder en *écriture* à des objets d'un niveau moins élevé

[a] Simple security rule
[b] $\star$-property

Muraille de chine

Modèle de Brewer & Nash

- basé sur l'histoire des accès
- combinaison de mandataire et de libre arbitre
- prévenir les conflits d'intérêt



Autorisations

- S peut lire O
  - si O est dans le même dataset qu'un objet auquel S a déjà accédé
  - *ou*, si O appartient à une classe de conflit à laquelle S n'a jamais accédé
- S peut écrire O
  - si S peut lire O
  - *et*, si S n'a jamais écrit dans un autre dataset que celui où il essaie d'écrire

Limitations

- gestion de l'historique,
- très restrictif.

Utilisation des vues

Types de privilèges SGBDR

- privilèges niveau système (opérations sur la base)
- privilèges niveau objet :
  - {SELECT, INSERT, UPDATE, ...} sur les *tables*.
  - {SELECT, INSERT, UPDATE, ...} sur les *vues*.

Possibilité d'utiliser les vues comme indirection !

```
GRANT <action> ON <objet> TO <sujet> [WITH GRANT OPTION]

    <action> ::= ALL |  SELECT | DELETE |
        INSERT [<attribut>]| UPDATE [<attribut>]|
        REFERENCE [<attribut>]
    <objet> ::= TABLE <relation> * | VIEW <vue> *
    <sujet> ::= PUBLIC| <sujet> *
```

Vers la flexibilité

Insuffisances des modèles classiques

- nouvelles dimensions,
- nouveaux usages,
- nouvelles organisations.

Vers de nouveaux modèles

- coût et flexibilité de l'administration,
- composition sur mesure,
- nouveaux objectifs

Contrôle d'accès à rôles

Limites des modèles existants

- systèmes avec de nombreux utilisateurs,
- systèmes avec de nombreux objets,
- organisations flexibles.

Approche

Politique proche de l'organisation qui l'utilise :

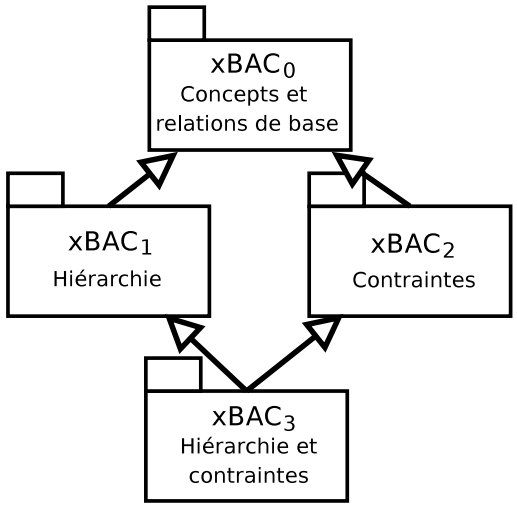
- RBAC est basé sur l'identification de rôles,
- les permissions sont associées aux rôles,
- les utilisateurs endossent des rôles aux travers de sessions.

Famille standard

Modèles standards

Plusieurs modèles RBAC définis dans le standard ANSI :

- RBAC_0 : le noyau,
- RBAC_1 : la hiérarchie,
- RBAC_2 : les contraintes,
- RBAC_3 : hiérarchies et contraintes.

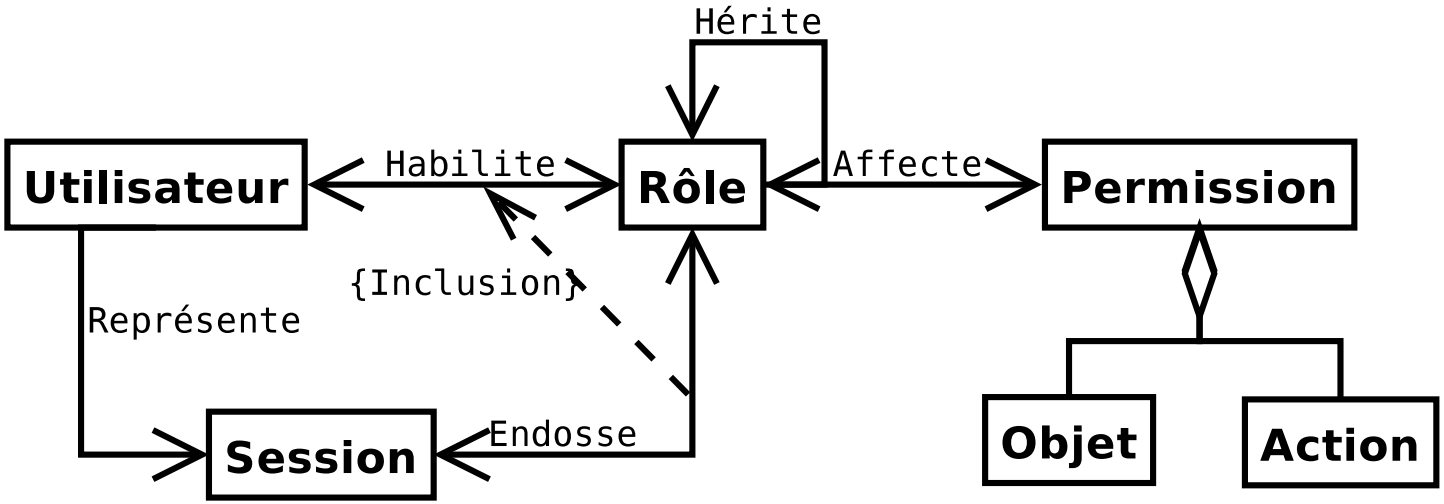


RBAC_0 et RBAC_1

> *. . . a job function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role.*

Distinction entre aspects :

- *statiques*,
- *dynamiques*.



Formalisation ensembliste

	Notation	Description
Concepts	$\mathcal{U}$	ensemble fini d'utilisateurs
	$\mathcal{R}$	ensemble fini de rôles
	$\mathcal{A}$	ensemble fini d'actions
	$\mathcal{O}$	ensemble fini d'objets
	$\mathcal{S}$	ensemble fini de sujets (sessions)
Relations	$\mathcal{P} \subseteq \mathcal{O} \times \mathcal{A}$	une action sur un objet
	$\mathcal{URA} \subseteq \mathcal{U} \times \mathcal{R}$	affectation de rôles aux utilisateurs
	$\mathcal{PRA} \subseteq \mathcal{R} \times \mathcal{P}$	affectation de permissions aux rôles
	$\mathcal{SU} \subseteq \mathcal{S} \times \mathcal{U}$	relation entre sessions et utilisateurs
	$\mathcal{SR} \subseteq \mathcal{S} \times \mathcal{R}$	relation entre sessions et rôles
	$\mathcal{RH} \subseteq \mathcal{R} \times \mathcal{R}$	relation d'héritage entre rôles

Exemple de politique

Politique RBAC : ▸ voir la matrice

- équivalente à la matrice jouet,
- cinq rôles sont définis,
- pas de hiérarchie.

URA

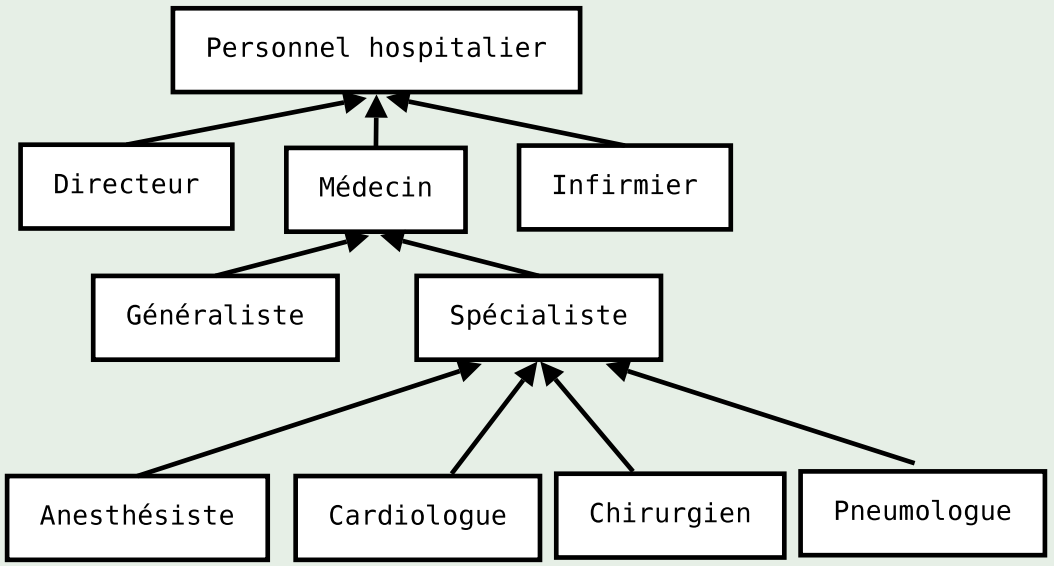
	I	M	G	P	S
Alice	×	×			
Bob	×		×		
Charly	×			×	
Denise					×

PRA

	r1	w1	**r2**	w2	**r3**	w3	r4	w4	x4
Infirmier	×		×		×				
Médecin		×							
Gastrologue				×			×	×	×
Pédiatre						×	×	×	×
Secrétaire					×		×		

Hiérarchisation des rôles

Une hiérarchie en arbre



Formes de hiérarchies

- arbre,
- arbre inverse,
- treillis,
- ordre partiel.

Formalisation ensembliste

Utilisateurs affectés et autorisés

$assigned\_users : \mathcal{R} \rightarrow 2^{\mathcal{U}}$ et $auth\_users : \mathcal{R} \rightarrow 2^{\mathcal{U}}$:

$$assigned\_users\ (\mathsf{r}) = \{u \in \mathcal{U} \mid (u, r) \in \mathcal{URA}\}$$

$$auth\_users\ (\mathsf{r}) = \{u \in \mathcal{U} \mid r' \succeq r \wedge (u, r') \in \mathcal{URA}\}$$

$$\forall r \in \mathcal{R}\ assigned\_users(r) \subseteq auth\_users(r)$$

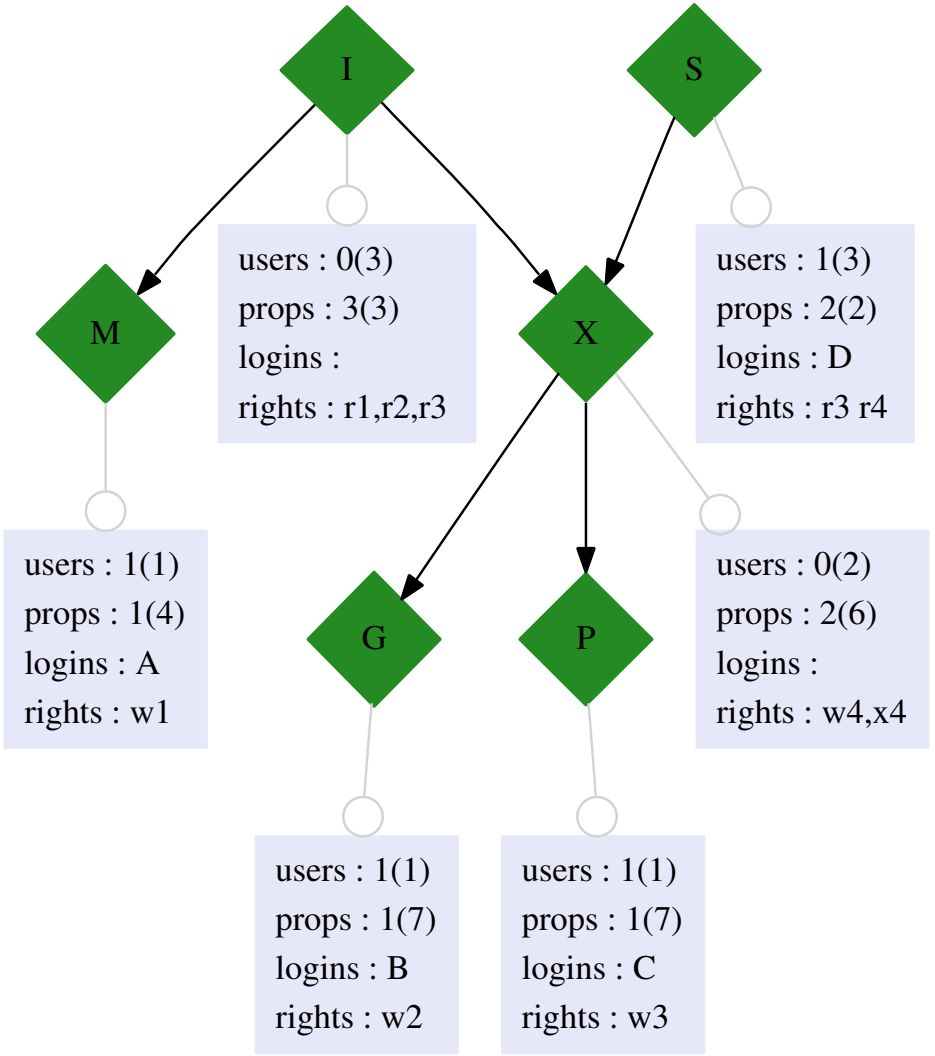
Permissions affectées et autorisées

$assigned\_perms : \mathcal{R} \rightarrow 2^{\mathcal{P}}$ et $auth\_perms : \mathcal{R} \rightarrow 2^{\mathcal{P}}$:

$$assigned\_perms\ (\mathsf{r}) = \{p \in \mathcal{P} \mid (r, p) \in \mathcal{PRA}\}$$

$$auth\_perms\ (\mathsf{r}) = \{p \in \mathcal{P} \mid r' \preceq r \wedge (r', p) \in \mathcal{PRA}\}$$

$$\forall r \in \mathcal{R}\ assigned\_perms(r) \subseteq auth\_perms(r)$$



Une hiérarchisation de la politique jouet

▸ voir la politique

Séparation des tâches

Principe de séparation des tâches

La *séparation des tâches* est un principe de sécurité qui impose que les acteurs qui interviennent dans la réalisation d'une tâche soient différents.

Réalisation

- Il faut qu'au moins n utilisateurs différents interviennent dans ce processus métier.
- Il ne peut pas y avoir $(n-1)$ utilisateurs qui disposent à eux seuls de l'ensemble des permissions pour effectuer l'ensemble du processus.

Dans RBAC_2

Contrainte d'exclusion

- *séparation des tâches* : un principe, *objectif* à garantir,
- *exclusion mutuelle* : une contrainte, un *moyen*.

Exclusion mutuelle entre rôles

- relation binaire interne $\mathcal{MER}$,
- symétrique et irréflexive,
- sémantiques multiples, confuses et dépendantes :
  - *User-based separation of duty*.
  - *Permission-based separation of duty*.
  - *Object-based separation of duty*.

Dans RBAC_3

Contraintes avec/sur la hiérarchie

- limites du standard,
- prérequis,
- spécialisation de l'héritage,

$$\forall r_1, r_2 \ (r_1, r_2) \in \mathcal{MER} \Rightarrow auth\_users(r_1) \cap auth\_users(r_2) = \emptyset$$

Interactions

- $\forall r_1, r_2 \ (r_1, r_2) \in \mathcal{MER} \Rightarrow \neg(r_1 \succeq r_2)$,
- $\forall r_1, r_2, r \ r \succeq r_1 \wedge r \succeq r_2 \Rightarrow (r_1, r_2) \notin \mathcal{MER}$,
- $\forall r_1, r_2, r \ (r_1, r_2) \in \mathcal{MER} \wedge r \succeq r_1 \Rightarrow (r, r_2) \in \mathcal{MER}$.

RBAC dans Oracle (1/3)

Gestion des rôles

- création de rôles,
- affectation/révocation $\mathcal{PRA}$,
- affectation/révocation $\mathcal{URA}$,
- activation de rôles $\mathcal{SR}$.

```
CREATE ROLE <role> [NOT IDENTIFIED | IDENTIFIED
  [BY <password> | EXTERNALLY]];

GRANT/REVOKE <role> TO <sujet>;
GRANT/REVOKE <role> TO <role>;

ALTER USER <user> DEFAULT ROLE [EXCEPT] [<role> * | NONE];

SET ROLE [EXCEPT] [<role> * | NONE];
```

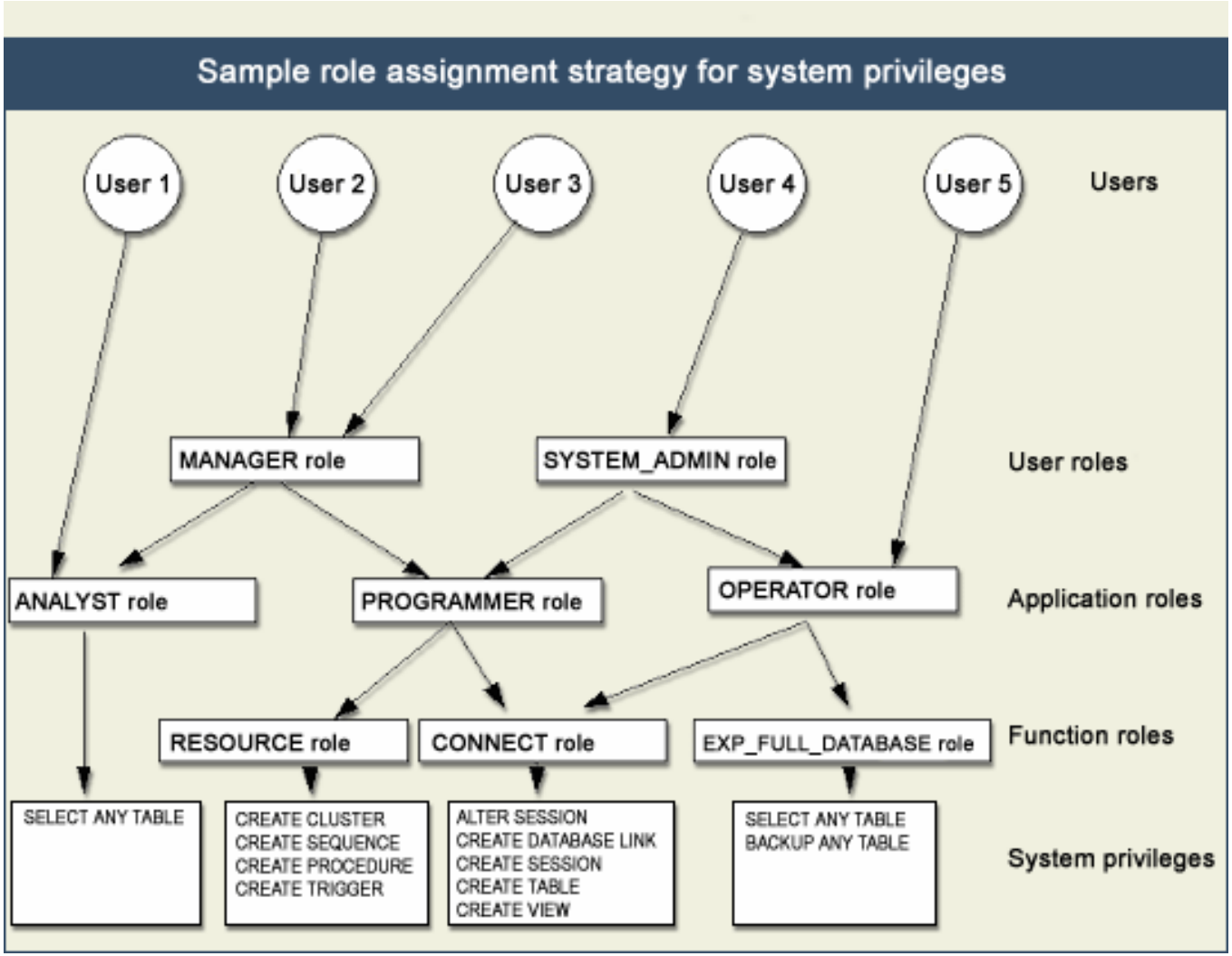
RBAC dans Oracle (2/3)

DBA_COL_PRIVS	Column object grants in the database.
DBA_ROLE_PRIVS	Roles granted to all users and roles
DBA_SYS_PRIVS	System priv. granted to users and roles.
DBA_TAB_PRIVS	Describes all object grants in the database.
DBA_TS_QUOTAS	Tablespace quotas for all users.
PRODUCT_PRIVS	Roles that are currently enabled.
ROLE_ROLE_PRIVS	Roles granted to other roles.
ROLE_SYS_PRIVS	System privileges granted to roles.
ROLE_TAB_PRIVS	Table privileges granted to roles.
SESSION_PRIVS	System privileges currently enabled.
COLUMN_PRIVILEGES	Depreciated use DBA_COL_PRIVS.
TABLE_PRIVILEGES	Depreciated use DBA_TAB_PRIVS.

Limites

- pas de contraintes de cardinalité
- pas de contraintes d'exclusion, ni statiques, ni dynamiques
- passage à l'échelle de la gestion des rôles

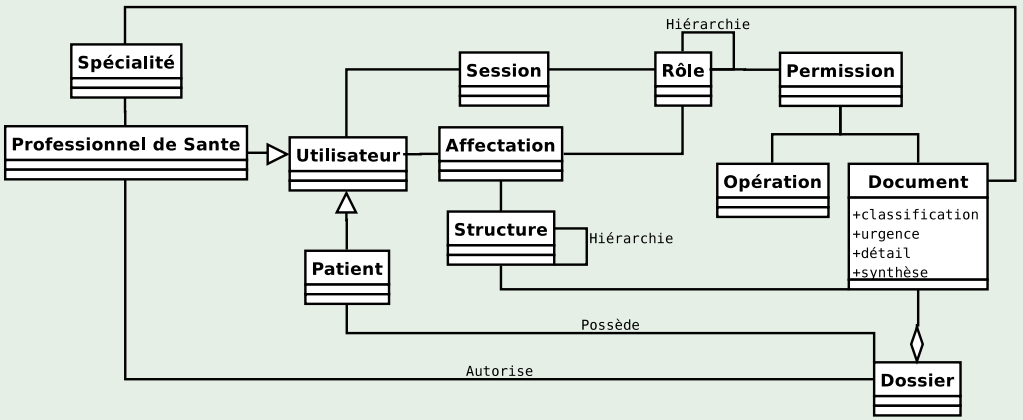
RBAC dans Oracle (3/3)



Concepts alternatifs

- tâches : *Task*-BAC,
- équipes : *Team*-BAC,
- espaces géographiques : *Geographical*-RBAC,
- dates & temps : *Temporal*-RBAC ...

Modèle composite

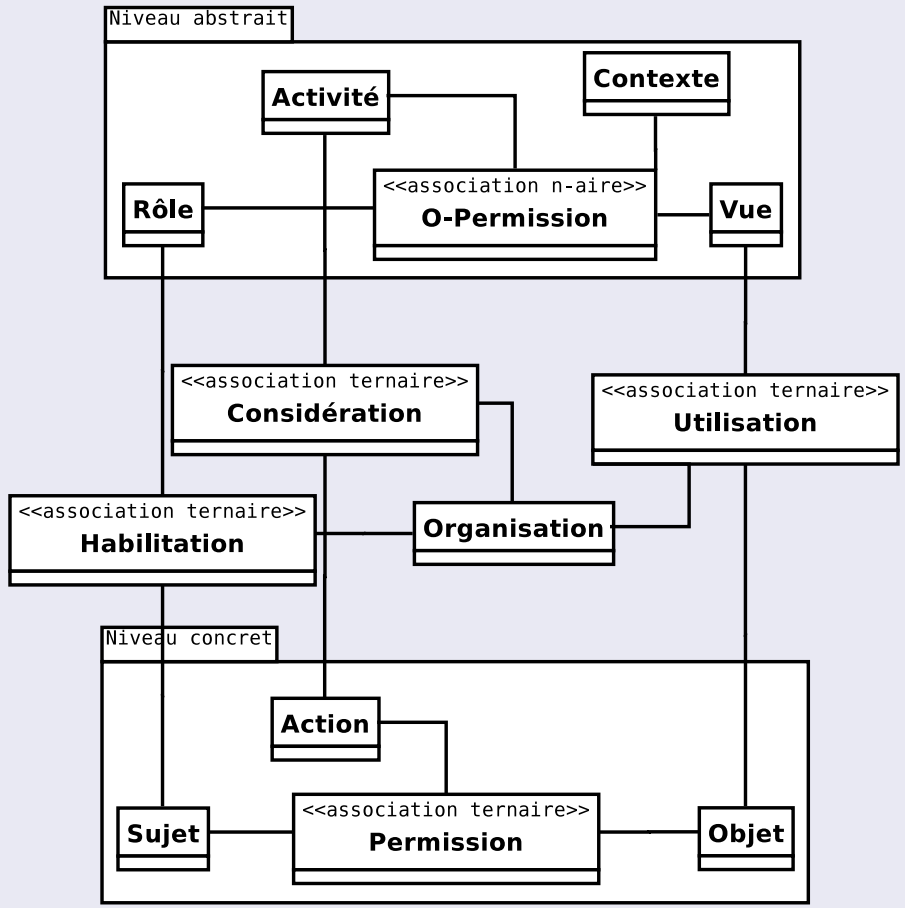


Modèle ORBAC

Principes

- Abstraction . . .
- & concrétisation,
- Orienté organisations,
- Relations ternaires.

Schéma



Thèmes de recherche

Problèmes connexes

- Authentification et son intégration,
- Contrôle de flux,
- Audit & conformité.

Autour du contrôle d'accès « pur »

- *Analyse* de politiques (cohérence, complétude),
- *Fouille et ingénierie* de politiques,
- *Délégation* et gestion de l'administration,
- Politiques distribuées.

Politiques distribuées

$$\mathcal{L} ::= \top \mid \phi \vee \psi \mid \phi \wedge \psi \mid \phi \rightarrow \psi \mid A \text{ says } \phi \mid X \mid \forall X.\phi$$

- $((A \text{ says } (\phi \rightarrow \psi)) \rightarrow (A \text{ says } \phi) \rightarrow (A \text{ says } \psi))$
- $\phi \rightarrow (A \text{ says } \phi)$
- $A \text{ says } (A \text{ says } \phi) \rightarrow (A \text{ says } \phi)$

Exemple

1. If *admin* says that *file* should be deleted, then this must be the case : $(admin \text{ says } delfile) \rightarrow delfile$
2. *admin* trusts *Bob* to decide whether *file* should be deleted : $admin \text{ says } ((Bob \text{ says } delfile) \rightarrow delfile)$
3. *Bob* wants to delete *file* : $Bob \text{ says } delfile$

Évolution des problématiques

Contrôle d'usage

- *Enterprise*-Digital Right Management,
- obligations dans le futur,
- modélisation des organisations et de leurs relations.

Protection de la vie privée

Contrôle d'accès *nécessaire* . . . mais pas *suffisant* !

- accès de la personne identifiée,
- retention limitée des données,
- proportionnalité et finalité des données,
- contrôle du transfert.

Grain à moudre


P. Samarati and S. D. C. di Vimercati. *Access control : Policies, models, and mechanisms.*
In *FOSAD '00*, pages 137–196, London, UK, 2001. Springer-Verlag.


N. Li, J. C. Mitchell. *DATALOG with constraints : A foundation for trust management languages*
In *PADL '03*, volume 2562 of *LNCS*, pages 58–73. 2003


S. Barker, P. J. Stuckey. *Flexible access control policy specification with constraint logic programming*
ACM Trans. Inf. Syst. Secur., 6(4) : 501–546, 2003.


J. Y. Halpern and V. Weissman. *Using first-order logic to reason about policies.*
ACM Trans. Inf. Syst. Secur., 11(4) :1–41, 2008.

Grain à moudre


D. Garg and M. Abadi. *A modal deconstruction of access control logics.*
FoSSaCS, volume 4962 of *LNCS*, pages 216–230. Springer, 2008.


X. Zhang, F. Parisi-Presicce, R. Sandhu, and J. Park. *Formal model and policy specification of usage control.*
ACM Trans. Inf. Syst. Secur., 8(4) :351–387, 2005.


C. M. Mathieu Jaume.*On specifying, implementing and comparing access control models. A semantical framework.*
Technical report, SPI - LIP6 - Universite Paris 6, France, 2008.


I. Molloy, H. Chen, T. Li, Q. Wang, N. Li, E. Bertino, S. Calo, S. Calo, and J. Lobo. *Mining roles with semantic meanings.*
In *SACMAT '08*, pages 21–30, New York, NY, USA, 2008. ACM.

Le mot de la fin

Kevin D. Mitnick – "*The Art of Deception*", p.79

> *Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people.*