

# Comparaison de modèles de contrôle d'accès

Mathieu Jaume

Université Paris 6 - LIP6

SSURF

25 Septembre 2007

# Le contrôle d'accès

---

## Définition

Le contrôle d'accès est n'importe quel mécanisme par lequel un système autorise ou interdit le droit à des entités actives (**sujets**) d'accéder à des entités passives (**objets**), ou d'effectuer des opérations.

# Le contrôle d'accès

---

## Définition

Le contrôle d'accès est n'importe quel mécanisme par lequel un système autorise ou interdit le droit à des entités actives (**sujets**) d'accéder à des entités passives (**objets**), ou d'effectuer des opérations.

- **Régir** les accès dans un système d'information  
Définir une **politique de sécurité** (i.e. spécifier quels sont les états du système qui satisfont la politique de contrôle d'accès considérée).

# Le contrôle d'accès

## Définition

Le contrôle d'accès est n'importe quel mécanisme par lequel un système autorise ou interdit le droit à des entités actives (**sujets**) d'accéder à des entités passives (**objets**), ou d'effectuer des opérations.

- **Régir** les accès dans un système d'information  
Définir une **politique de sécurité** (i.e. spécifier quels sont les états du système qui satisfont la politique de contrôle d'accès considérée).
- **Gérer** les accès dans un système d'information  
Définir un **moniteur de référence** permettant de mettre en application la politique (i.e. un programme qui autorise ou refuse les accès demandés par les sujets sur les objets).

# Objectifs

---

**Objectif à “long” terme** : Développement formel d'une bibliothèque implantant des politiques de contrôle d'accès

# Objectifs

---

**Objectif à “long” terme** : Développement formel d'une bibliothèque implantant des politiques de contrôle d'accès

- Formaliser la politique, Mécaniser la formalisation
- Modifier une partie de la spécification ? Faciliter la réutilisation

Travailler dans un cadre générique

# Objectifs

---

**Objectif à "long" terme** : Développement formel d'une bibliothèque implantant des politiques de contrôle d'accès

- Formaliser la politique, Mécaniser la formalisation
- Modifier une partie de la spécification ? Faciliter la réutilisation  
Travailler dans un cadre générique
- Algèbre des modèles de contrôle d'accès de McLean.
  - ▶ trop contraignante : le paramètre de sécurité n'est pas forcément un treillis de niveaux de sécurité (ex : Muraille de Chine, RBAC, ...)
  - ▶ pas assez expressive (comparaison de politiques et d'implantations)

# Objectifs

**Objectif à “long” terme** : Développement formel d'une bibliothèque implantant des politiques de contrôle d'accès

- Formaliser la politique, Mécaniser la formalisation
- Modifier une partie de la spécification ? Faciliter la réutilisation  
Travailler dans un cadre générique
- Algèbre des modèles de contrôle d'accès de McLean.
  - ▶ trop contraignante : le paramètre de sécurité n'est pas forcément un treillis de niveaux de sécurité (ex : Muraille de Chine, RBAC, ...)
  - ▶ pas assez expressive (comparaison de politiques et d'implantations)
- Définition d'un cadre sémantique générique permettant de spécifier, d'implanter et de comparer des modèles de contrôle d'accès.

# Politique de contrôle d'accès

Régir les accès dans un système d'information

## Définition

$$\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$$

- $\mathcal{S}$  et  $\mathcal{O}$  : Ensembles de sujets et d'objets.
- $\mathcal{A}$  : Ensemble de modes d'accès (lecture, écriture, ...)
- $\rho$  : Paramètres de sécurité (treillis de niveau de sécurité, classes de conflit d'intérêt, ...)
- $\Sigma$  : Ensemble d'états du système sur lequel la politique de sécurité est mise en oeuvre.
- $\Omega$  : Prédicat de sécurité que doivent vérifier les états sûrs du système.

# Etats

---

Etat  $\sigma \in \Sigma$  :

- $\Upsilon(\sigma)$  : **fonctions de sécurité**, qui associent aux sujets et objets des informations construites à partir des paramètres de sécurité  $\rho$ .
- $\Lambda(\sigma) \in \wp(\mathbb{A})$  : **ensemble d'accès courants**, qui décrit tous les accès en cours. Un accès est généralement vu comme un triplet (sujet, objet, mode d'accès) ... mais d'autres choix sont possibles.

# Etats

Etat  $\sigma \in \Sigma$  :

- $\Upsilon(\sigma)$  : **fonctions de sécurité**, qui associent aux sujets et objets des informations construites à partir des paramètres de sécurité  $\rho$ .
- $\Lambda(\sigma) \in \wp(\mathbb{A})$  : **ensemble d'accès courants**, qui décrit tous les accès en cours. Un accès est généralement vu comme un triplet (sujet, objet, mode d'accès) ... mais d'autres choix sont possibles.
- Observateur d'état  
 $\mathcal{W}(\sigma)$  : ensembles d'accès que l'on peut ajouter aux accès courants de  $\sigma$  tout en préservant la politique.

$$\mathcal{W}(\sigma) = \left\{ A \subseteq \wp(\mathbb{A}) \mid \forall \sigma' \in \Sigma \right. \\ \left. (\Upsilon(\sigma') = \Upsilon(\sigma) \wedge \Lambda(\sigma') = \Lambda(\sigma) \cup A) \Rightarrow \Omega(\sigma') \right\}$$

# Politiques compactes

---

$\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$  est **compacte** ssi supprimer des accès courants à un état sûr préserve la politique.

$$\forall \sigma_1 \in \Sigma \quad \Omega(\sigma_1) \Rightarrow (\forall \sigma_2 \in \Sigma \quad (\Lambda(\sigma_2) \subseteq \Lambda(\sigma_1) \wedge \Upsilon(\sigma_1) = \Upsilon(\sigma_2)) \Rightarrow \Omega(\sigma_2))$$

# Politiques compactes

$\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$  est **compacte** ssi supprimer des accès courants à un état sûr préserve la politique.

$$\forall \sigma_1 \in \Sigma \quad \Omega(\sigma_1) \Rightarrow (\forall \sigma_2 \in \Sigma (\Lambda(\sigma_2) \subseteq \Lambda(\sigma_1) \wedge \Upsilon(\sigma_1) = \Upsilon(\sigma_2)) \Rightarrow \Omega(\sigma_2))$$

*Exemple de politique non compacte* : un sujet ne peut accéder à une ressource d'un autre domaine que le sien uniquement si toutes les ressources de son domaine sont déjà accédées.

# Exemples de politiques

---

$$\mathbb{P}_{ACL}[\rho_{ACL}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{ACL}, \Omega_{ACL})$$

Politique discrétionnaire

---

$$\mathbb{P}_{BLP}[\rho_{BLP}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{BLP}, \Omega_{BLP})$$

Politique de Bell et LaPadula

---

$$\mathbb{P}_{RBLP}[\rho_{RBLP}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{RBLP}, \Omega_{RBLP})$$

Interprétation à base de rôles de la Politique de Bell et LaPadula

---

$$\mathbb{P}_{RBAC}[\rho_{RBAC}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{RBAC}, \Omega_{RBAC})$$

Politique à base de rôles

---

$$\mathbb{P}_{CW}[\rho_{CW}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{CW}, \Omega_{CW})$$

Politique de la muraille de Chine

---

$$\mathbb{P}_{LCW}[\rho_{LCW}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{LCW}, \Omega_{LCW})$$

Interprétation à base de treillis de la Politique de la muraille de Chine

# Exemples de politiques

---

$$\mathbb{P}_{ACL}[\rho_{ACL}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{ACL}, \Omega_{ACL})$$

Politique discrétionnaire

---

$$\mathbb{P}_{BLP}[\rho_{BLP}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{BLP}, \Omega_{BLP})$$

Politique de Bell et LaPadula

---

$$\mathbb{P}_{RBLP}[\rho_{RBLP}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{RBLP}, \Omega_{RBLP})$$

Interprétation à base de rôles de la Politique de Bell et LaPadula

---

$$\mathbb{P}_{RBAC}[\rho_{RBAC}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{RBAC}, \Omega_{RBAC})$$

Politique à base de rôles

---

$$\mathbb{P}_{CW}[\rho_{CW}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{CW}, \Omega_{CW})$$

Politique de la muraille de Chine

---

$$\mathbb{P}_{LCW}[\rho_{LCW}] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_{LCW}, \Omega_{LCW})$$

Interprétation à base de treillis de la Politique de la muraille de Chine

**Proposition.**  $\mathbb{P}_{ACL}[\rho_{ACL}]$ ,  $\mathbb{P}_{BLP}[\rho_{BLP}]$ ,  $\mathbb{P}_{RBLP}[\rho_{RBLP}]$ ,  $\mathbb{P}_{RBAC}[\rho_{RBAC}]$ ,  $\mathbb{P}_{CW}[\rho_{CW}]$  et  $\mathbb{P}_{LCW}[\rho_{LCW}]$  sont des politiques compactes.



# Requêtes

---

**Gérer** les accès dans un système d'information

*Décrire l'implantation de politiques de contrôle d'accès*

# Requêtes

**Gérer** les accès dans un système d'information

*Décrire l'implantation de politiques de contrôle d'accès*

$\mathcal{R}$  : Ensemble de requêtes.

*Exemples :*

- **Requêtes sur les accès** : modification de  $\Lambda(\sigma)$

$\{\langle +, s, o, \text{read} \rangle, \langle +, s, o, \text{write} \rangle, \langle -, s, o, \text{read} \rangle, \langle -, s, o, \text{write} \rangle\}$

- **Requêtes administratives** : modification de  $\Upsilon(\sigma)$

Ajout d'un rôle, changement d'un niveau de sécurité, ...

# Sémantique des requêtes

Etant donné une politique  $\mathbb{P}[\rho]$ , la sémantique des requêtes est définie par

- une relation :

$$\llbracket \mathcal{R} \rrbracket_{\Sigma} \subseteq \mathcal{R} \times \Sigma$$

*Exemple :*  $(\langle +, s, o, \text{read} \rangle, \sigma) \in \llbracket \mathcal{R} \rrbracket_{\Sigma} \Leftrightarrow (s, o, \text{read}) \in \Lambda(\sigma)$

# Sémantique des requêtes

Etant donné une politique  $\mathbb{P}[\rho]$ , la sémantique des requêtes est définie par

- une relation :

$$\llbracket \mathcal{R} \rrbracket_{\Sigma} \subseteq \mathcal{R} \times \Sigma$$

*Exemple :*  $(\langle +, s, o, \text{read} \rangle, \sigma) \in \llbracket \mathcal{R} \rrbracket_{\Sigma} \Leftrightarrow (s, o, \text{read}) \in \Lambda(\sigma)$

- un partitionnement des requêtes :  $\mathcal{R} = \mathcal{R}^{\ominus} \cup \mathcal{R}^{\oplus} \cup \mathcal{R}^{\circ}$

# Sémantique des requêtes

Etant donné une politique  $\mathbb{P}[\rho]$ , la sémantique des requêtes est définie par

- une relation :

$$\llbracket \mathcal{R} \rrbracket_{\Sigma} \subseteq \mathcal{R} \times \Sigma$$

*Exemple :*  $(\langle +, s, o, \text{read} \rangle, \sigma) \in \llbracket \mathcal{R} \rrbracket_{\Sigma} \Leftrightarrow (s, o, \text{read}) \in \Lambda(\sigma)$

- un partitionnement des requêtes :  $\mathcal{R} = \mathcal{R}^{\ominus} \cup \mathcal{R}^{\oplus} \cup \mathcal{R}^{\circ}$

*Exemples*

- ▶  $(\langle +, s, o, \text{read} \rangle, \sigma) \in \mathcal{R}^{\ominus}$  pour  $\mathbb{P}_{BLP}[\rho_{BLP}]$  et  $\mathbb{P}_{CW}[\rho_{CW}]$
- ▶ “Requête d’ajout d’un rôle à un sujet”  $\in \mathcal{R}^{\oplus}$  pour  $\mathbb{P}_{RBAC}[\rho_{RBAC}]$

# Modèle de contrôle d'accès

## Definition

$$M[\rho] = (\mathbb{P}[\rho], \llbracket \mathcal{R} \rrbracket_{\Sigma})$$

- $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$  : Politique de sécurité.
- $\mathcal{R}$  : Ensemble de requêtes.
- $\llbracket \mathcal{R} \rrbracket_{\Sigma}$  : Sémantique des requêtes.

# Implantations

---

- Une implantation d'un modèle est une paire  $(\tau, \Sigma_I)$  :

$$\tau : \mathcal{R} \times \Sigma \rightarrow \mathcal{D} \times \Sigma \quad \Sigma_I \subseteq \Sigma$$

# Implantations

- Une implantation d'un modèle est une paire  $(\tau, \Sigma_I)$  :

$$\tau : \mathcal{R} \times \Sigma \rightarrow \mathcal{D} \times \Sigma \quad \Sigma_I \subseteq \Sigma$$

## Propriétés sur les implantations

- Correction par rapport à la politique de sécurité.
- Correction par rapport à la sémantique des requêtes.
- Correction par rapport à la partition des requêtes.

# Implantations - Exemples

- Modèle **discrétionnaire**  $\mathbb{M}_{ACL}[\rho_{ACL}] \vdash (\tau_{ACL}, \Sigma_I^{ACL})$
- Modèle de **Bell et LaPadula**  $\mathbb{M}_{BLP}[\rho_{BLP}] \vdash (\tau_{BLP}, \Sigma_I^{BLP})$
- Modèle de la **Muraille de Chine**  $\mathbb{M}_{CW}[\rho_{CW}] \vdash (\tau_{CW}, \Sigma_I^{CW})$
- Modèle **RBAC**  $\mathbb{M}_{RBAC}[\rho_{RBAC}] \vdash (\tau_{RBAC}, \Sigma_I^{RBAC})$

# Comparaison d'implantations

---

- Il existe plusieurs implantations plus ou moins restrictives d'une même politique.

$$\forall R \forall \sigma \tau_{no}(R, \sigma) = (no, \sigma)$$

# Comparaison d'implantations

- Il existe plusieurs implantations plus ou moins restrictives d'une même politique.

$$\forall R \forall \sigma \tau_{no}(R, \sigma) = (no, \sigma)$$

- *Comparaison des implantations d'une même politique*

$I \sqsubseteq I'$  ssi :

- ▶ les états accessibles avec  $I$  le sont également avec  $I'$ ,
- ▶  $I'$  permet de faire de "plus petits pas" que  $I$ .

# Comparaison de modèles

---

- $M_1[\rho_1]$  est plus “petit” que  $M_2[\rho_2]$  si tout ce qui peut être “fait” avec  $M_1[\rho_1]$  peut l’être également avec  $M_2[\rho_2]$

# Comparaison de modèles

- $M_1[\rho_1]$  est plus “petit” que  $M_2[\rho_2]$  si tout ce qui peut être “fait” avec  $M_1[\rho_1]$  peut l’être également avec  $M_2[\rho_2]$

## Definition (Préordre sur les modèles)

$M_1[\rho_1]$  est plus restrictif que  $M_2[\rho_2]$  ssi toute implantation correcte de  $M_1[\rho_1]$  peut être simulée par une implantation correcte de  $M_2[\rho_2]$  ... via une relation de simulation qui satisfait de bonnes propriétés.

# Modèles réduits

## Réduction d'un modèle

On regroupe les états “équivalents” ...

On introduit une relation d'équivalence sur les états :

- $\sigma_1 \equiv_{\mathcal{W}} \sigma_2 \Leftrightarrow \mathcal{W}(\sigma_1) = \mathcal{W}(\sigma_2)$
- $\sigma_1 \equiv_{\mathcal{W}_\emptyset} \sigma_2 \Leftrightarrow \mathcal{W}_\emptyset(\sigma_1) = \mathcal{W}_\emptyset(\sigma_2)$
- $\sigma_1 \equiv_{\mathcal{R}} \sigma_2 \Leftrightarrow (\forall R \in \mathcal{R} (\sigma_1, R) \in \llbracket \mathcal{R} \rrbracket_\Sigma \Leftrightarrow (\sigma_2, R) \in \llbracket \mathcal{R} \rrbracket_\Sigma)$

## Relation d'équivalence

$$\sigma_1 \equiv_l \sigma_2 \Leftrightarrow (\sigma_1 \equiv_{\mathcal{W}} \sigma_2 \wedge \sigma_1 \equiv_{\mathcal{W}_\emptyset} \sigma_2 \wedge \sigma_1 \equiv_{\mathcal{R}} \sigma_2)$$

**Réduction/Concrétisation de modèles, d'implantations ...**

# Comparaison de modèles

---

## Problème 1

Il existe beaucoup d'implantations de  $M_1[\rho_1]$ . Comment limiter le nombre d'implantations à considérer ?

# Comparaison de modèles

## Problème 1

Il existe beaucoup d'implantations de  $M_1[\rho_1]$ . Comment limiter le nombre d'implantations à considérer ?

## Proposition 1

$M_1[\rho_1]$  est plus restrictif que  $M_2[\rho_2]$  ssi on sait construire une relation de simulation qui préserve les politiques (prédicats  $\Omega_1$  et  $\Omega_2$ ) ainsi que la sémantique des requêtes.

# Comparaison de modèles

## Problème 1

Il existe beaucoup d'implantations de  $\mathbb{M}_1[\rho_1]$ . Comment limiter le nombre d'implantations à considérer ?

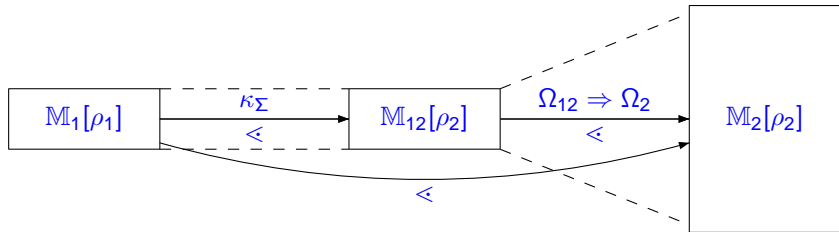
## Proposition 1

$\mathbb{M}_1[\rho_1]$  est plus restrictif que  $\mathbb{M}_2[\rho_2]$  ssi on sait construire une relation de simulation qui préserve les politiques (prédicats  $\Omega_1$  et  $\Omega_2$ ) ainsi que la sémantique des requêtes.

## Proposition 2

$\mathbb{M}_1[\rho_1]$  est plus restrictif que  $\mathbb{M}_2[\rho_2]$  ssi les implantations les “moins restrictives” de  $\mathbb{M}_1[\rho_1]$  peuvent être simulées par des implantations de  $\mathbb{M}_2[\rho_2]$ .

# Applications (1)



## Applications (2)

- $\rho_2 = f(\rho_1)$  et on montre  $\forall \rho_1 \quad \exists \rho_2 \quad \mathbb{M}_1[\rho_1] \triangleleft \mathbb{M}_2[\rho_2]$ 
  - $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{LCW}[\rho_{LCW}] \triangleleft \mathbb{M}_{BLP}[\rho_{LCW}]$
  - $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{BLP}[\rho_{LCW}]$
  - $\mathbb{M}_{BLP}[\rho_{BLP}] \triangleleft \mathbb{M}_{RBLP}[\rho_{RBLP}] \triangleleft \mathbb{M}_{RBAC}[\rho_{RBLP}]$
  - $\mathbb{M}_{BLP}[\rho_{BLP}] \triangleleft \mathbb{M}_{RBAC}[\rho_{RBLP}]$

- on montre ...

$$\mathbb{M}_{BLP}[\rho_{BLP}] \not\triangleleft \mathbb{M}_{CW}[\rho_{CW}]$$
$$\mathbb{M}_{RBAC}[\rho_{RBAC}] \not\triangleleft \mathbb{M}_{BLP}[\rho_{BLP}]$$

## Conclusion, Travaux en cours, Travaux futurs ...

---

- Cadre sémantique générique pour spécifier, implanter et comparer des politiques de contrôle d'accès.
- Outil pour mieux comprendre ces politiques

# Conclusion, Travaux en cours, Travaux futurs ...

- Cadre sémantique générique pour spécifier, implanter et comparer des politiques de contrôle d'accès.
- Outil pour mieux comprendre ces politiques
- Implantation avec l'atelier FOCAL
- Comparaisons : Travaux parcellaires
  - ▶ en terme de simulation
  - ▶ en terme de puissance d'expression
  - ▶ en terme de combinaisons de politiques
  - ▶ ...

Comparer  $\sqsubseteq$  avec les "comparaisons" existantes

- Composition de politiques de sécurité  
Différentes manières de composer des politiques, Recensement  
Cadre pour exprimer formellement les compositions