Etude formelle de systèmes de contrôle d'accès

Journée des Doctorants LIP6 - LTCI - EDITE

Lionel Habib

SPI - LIP6 - UPMC

1er Octobre 2008

Direction : Thérèse Hardin
Mathieu Jaume

Equipe SPI

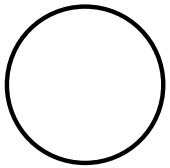
- Développement de l'atelier FoCaL au sein de l'équipe SPI-LIP6
  - Développé en partenariat avec le CEDRIC-CNAM et l'INRIA
- Domaine de recherche : Approche formelle de la sécurité et de la sûreté de fonctionnement
  - Travaux de thèse : Méthodes formelles appliquées au contrôle d'accès
- Travaux réalisés dans le cadre du projet ANR-SSURF (Safety and Security UndeR Focal)

Bibliothèque certifiée de modèles de contrôle d'accès

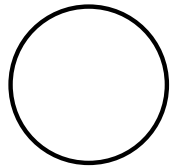
- Développée avec l'atelier FoCaL :
  - Langage fonctionnel muni de traits objets
    - ★ compilé vers OCaml et Coq
  - Langage d'expressions logiques
    - ★ compilé vers Coq
  - Langage de preuve couplé au prouveur Zenon
    - ★ compilé vers Coq
- Comprend les modèles Bell & LaPadula, RBAC, HRU, Mécanismes de Délégation, Unix, Tickets inforgeables

Contrôle d'accès

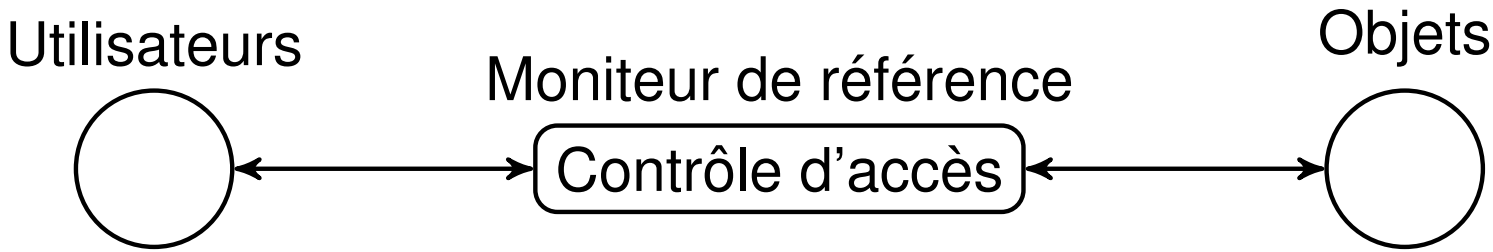
Utilisateurs



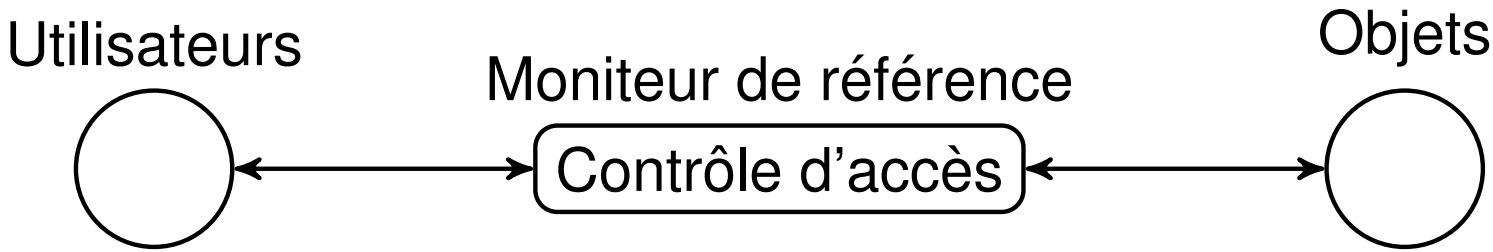
Objets



Contrôle d'accès



Contrôle d'accès



- Un système de contrôle d'accès repose sur deux concepts principaux :
  - La politique de contrôle d'accès
  - Le moniteur de référence

Formalisation du contrôle d'accès

- Cadre générique permettant d'exprimer formellement des modèles de contrôle d'accès
  - Fournit une méthodologie de formalisation
- Objectifs :
  - Definir une sémantique pour les systèmes de contrôle d'accès
  - Identifier des propriétés générales sur les modèles de contrôle d'accès
  - Comparer des modèles de contrôle d'accès
  - Composer des modèles de contrôle d'accès
  - Factoriser une partie des implantations

Comparaison de modèles de contrôle d'accès

- Mécanisme de comparaison basé sur la notion de simulation de fonctions de transition
- Un modèle $\mathbb{M}_1$ est plus restrictif qu'un modèle $\mathbb{M}_2$ ($\mathbb{M}_1 \trianglelefteq \mathbb{M}_2$) si et seulement si tout moniteur de référence de $\mathbb{M}_1$ peut-être simulé par un moniteur de référence de $\mathbb{M}_2$
- Résultats théoriques permettant de faciliter la comparaison de deux modèles
- Classification de modèles courants :

$$\mathbb{M}_{cw} \triangleleft \mathbb{M}_{blp} \triangleleft \mathbb{M}_{rbac} \equiv \mathbb{M}_{hru}$$

Composition de modèles de contrôle d'accès

- Qu'est-ce que composer des modèles de contrôle d'accès ?
- Comment composer des modèles de contrôle d'accès ?
- Quelles sont les classes d'opérateurs de composition ?
- Quelles propriétés ces opérateurs garantissent ?
- Quelle est la sémantique de chaque opérateur ?