

Contrôles d'Accès Sécurisés à des données Confidentielles

Evolution des systèmes d'information

- Evolution des sources d'information
 - Largement distribuées, autonomes, hétérogènes
- Evolution des modèles de données
 - Données semi-structurées, arborescentes
- Evolution des modes d'accès à l'information
 - Accès ubiquitaire, Push, P2P...
- Apparition du contrôle d'usage
 - Exemple : Digital Right Management (DRM)

→ Comment exprimer les droits d'accès et d'usage ?

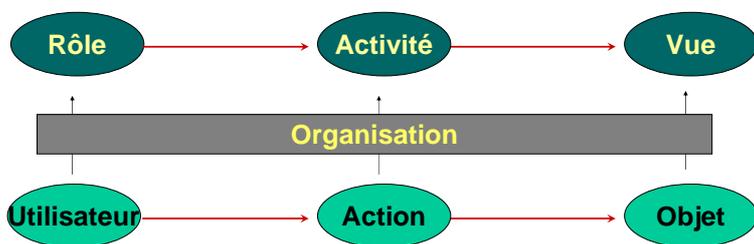
Sources de vulnérabilité

- Contournement de droits
 - Attaques de l'empreinte disque
 - Vulnérabilité des serveurs d'entreprise
 - Attaques internes (e.g. rapport CSI/FBI)
- Détournement de droits
 - Violation de chartes de confidentialité (e.g., rapport IBM-Harris)

→ Comment garantir le respect des droits (accès / usage)?

Objectifs de CASC

1. Abstraction des concepts à intégrer dans les modèles de droits d'accès, formalisation des procédures d'administration.
2. Définition d'un modèle de droits d'accès puissant et cohérent pour documents XML.
3. Sécurisation matérielle des données, du contrôle des droits et de leur administration.

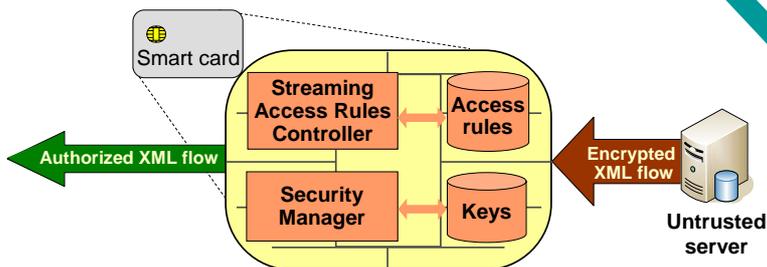
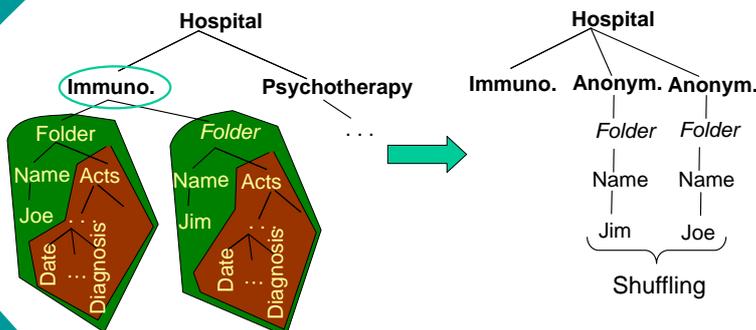


1 - Or-BAC, AdOr-BAC

- Droits de type :
 - Right (Organisation, Role, Activity, View, Context)
- Modèle d'auto-administration AdOr-BAC
 - Exprimé avec les entités Or-BAC
- Application aux droits digitaux (e.g., MPEG-REL)

2 - Contrôle d'accès XML

- Modèle intégrant les droits sur les liens
 - Vue autorisée = restructuration du document source
- Modèle incluant les privilèges en modification
 - Support du langage Xupdate
- Analyses de sécurité de transformations XML



3 - Sécurisation du Contrôle

- Sécurisation du contrôle pour des docs XML
 - Traitement en flux dans une carte à puce
 - Index spécifique maximisant les performances
- Application à un modèle « DRM équitable »
 - Accès en fonction du profil de l'utilisateur.
 - Gold Award du concours SIMagine 2005