ACI Sécurité Informatique

C.A.S.C

Contrôles d'Accès Sécurisés à des données Confidentielles

(2003-2006)

Participants : INRIA, ENS, ENST Bretagne, LRI, LIUPPA

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 ?

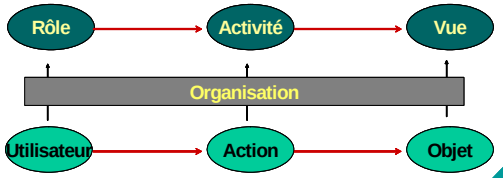
Sources de vulnérabilité

- **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 privacité (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.**

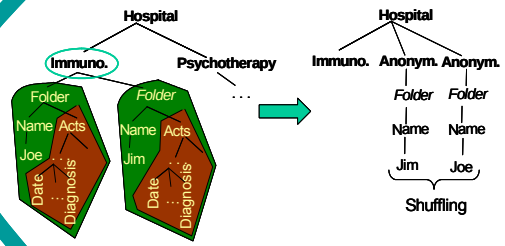


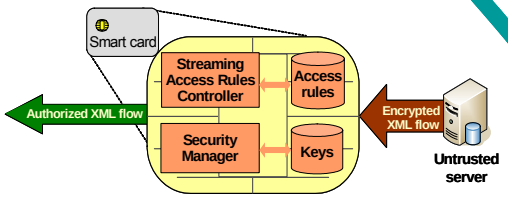
1 - Or-BAC, AdOr-BAC

- **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

ACI Sécurité Informatique
C.A.S.C (2003-2006)

Contact : Luc Bouganim
E-mail : Luc.Bouganim@inria.fr
http://www-smis.inria.fr/~bouganim/CASC/

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 ?

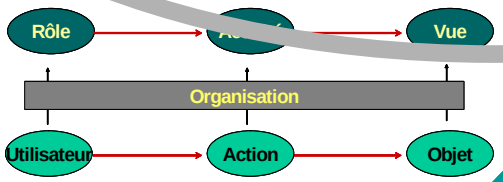
Sources de vulnérabilité

- **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 privacité (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.**

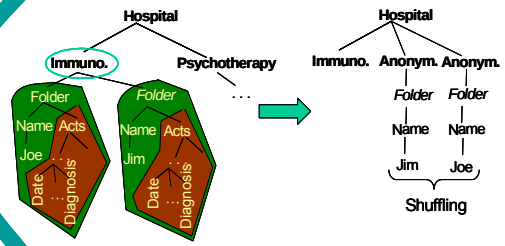


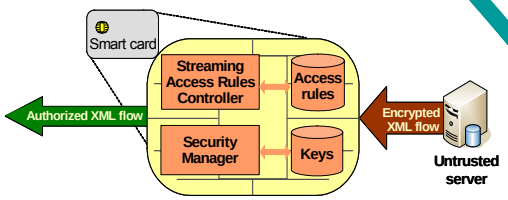
1 - Or-BAC, AdOr-BAC

- **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**





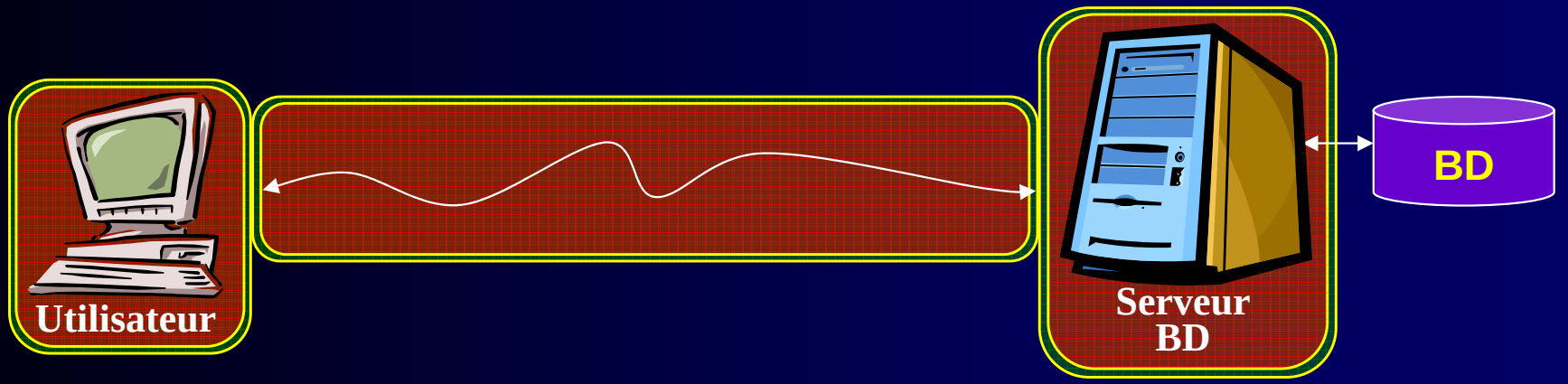
3 - Sécurisation du Contrôle

- **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

ACI Sécurité Informatique
C.A.S.C (2003-2006)

Contact : Luc Bouganim
E-mail : Luc.Bouganim@inria.fr
http://www-smis.inria.fr/~bouganim/CASC/

Confidentialité dans les SGBD



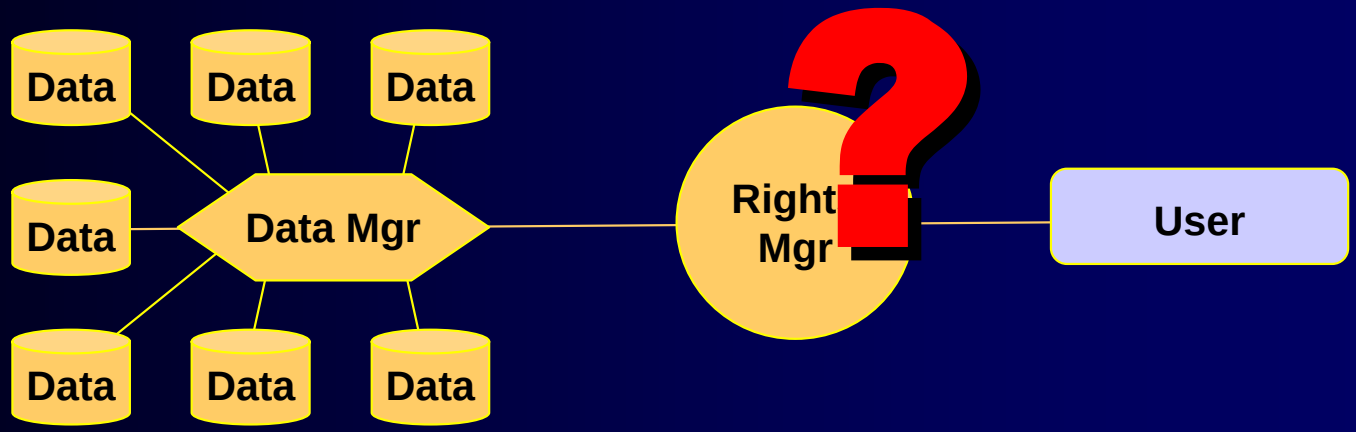
- **Identification / authentification**
- **Chiffrement des communications**
- **Contrôle d'accès sur le serveur**
  - Autorisations définies sur n'importe quel objet de la BD
    - N'importe quel granularité
    - Peuvent être définies sur des objets **virtuels** (i.e., données calculées)

Contexte : Evolution des systèmes d'information

- **Evolution des sources d'information**
  - BDs centralisées → Sources de données largement distribuées, autonomes, hétérogènes
- **Evolution des modèles de données**
  - Tabulaires, structurées → semi-structurées, arborescentes
- **Evolution des modes d'accès à l'information**
  - Client/serveur → accès ubiquitaire, Push, P2P…
- **Apparition du contrôle d'*usage***
  - Contrôle d'accès → Contrôle d'usage
    - Exemple : Digital Right Management (DRM)

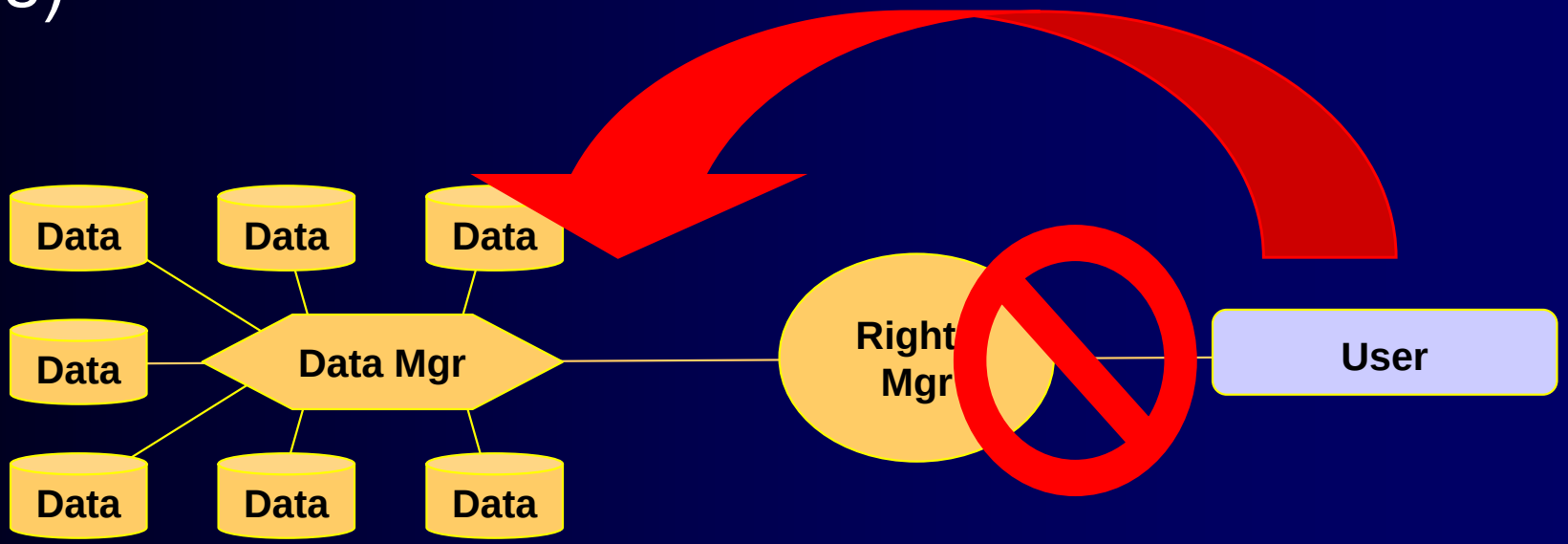
Exprimer les droits d'accès et d'usage ?

- **Les modèles existants sont inadaptés**
  - à la distribution, l'autonomie, l'hétérogénéité des sources de données
  - aux nouveaux modèles de données (XML)
  - aux différents modes d'accès
  - au contrôle d'usage

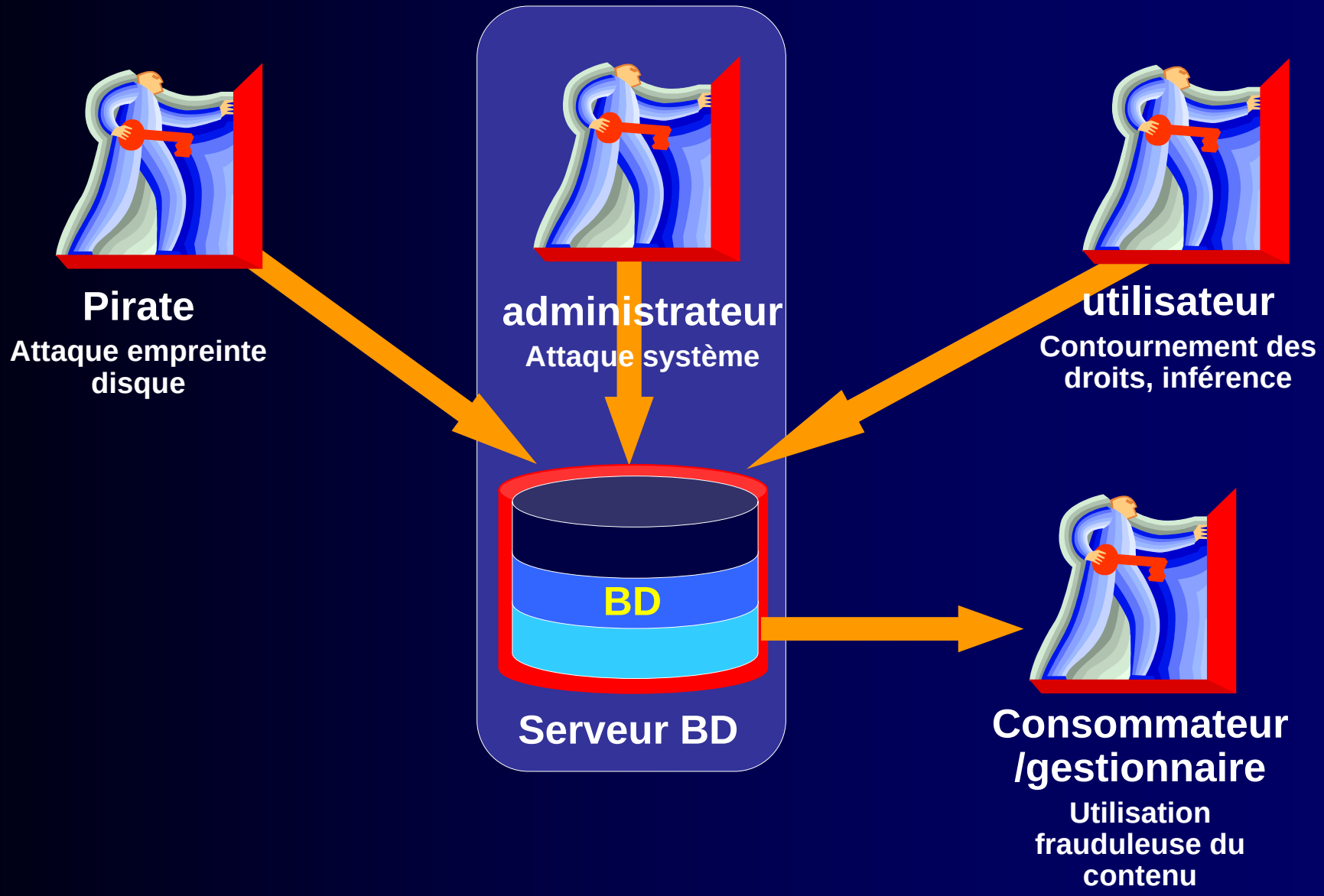


Comment garantir le respect des droits ?

- **Contournement de droits**
  - Attaques de l'empreinte disque
  - Attaques internes (e.g. rapport CSI/FBI)
- **Détournement de droits**
  - Violation de chartes de privacité (e.g., rapport IBM-Harris)



Attaques sur les données…



Objectifs de l'ACI CASC

1. Abstraction des concepts à intégrer dans les modèles de droits d'accès et formalisation des procédures d'administration associées,

2. Définition de modèles de droits d'accès puissants et cohérents pour documents XML,

3. Sécurisation matérielle des données, du contrôle des droits et de leur administration.

➔ l'ACI CASC est organisée en 3 tâches relatives à ces trois objectifs

Participants

 Projet SMIS	**Luc Bouganim**	CR (Coordinateur)	**Sécurisation matérielle du contrôle d'accès et d'usage**
	Philippe Pucheral	PR-UVSQ (détach^{t} INRIA)	
	François Dang Ngoc	Doctorant	
 Equipe SERES	**Frédéric Cuppens**	PR	**Formalisation des modèles de contrôle d'accès et d'administration**
	Sylvain Gombault	MC	
	Nora Cuppens	IR	
	Thierry Sans	Doctorant	
 Equipe CSySEC	**AlbanGabillon**	PR	**Modèles de contrôle d'accès pour documents XML**
	Janvier Majirus Fansi	Doctorant	
 LIENS	**Giuseppe Castagna**	CR-CNRS (ENS)	**Analyse de la sécurité de transformations XML**
	Veronique Benzaken	PR (LRI)	
	Darlo Colazzo	Post-Doc (LRI)	
	Marwan Burelle	Doctorant (LRI)	

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 ?

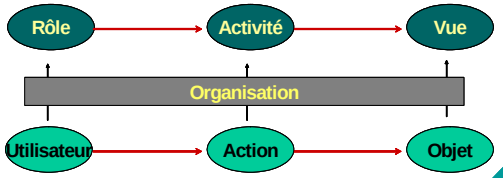
Sources de vulnérabilité

- **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 privacité (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.**

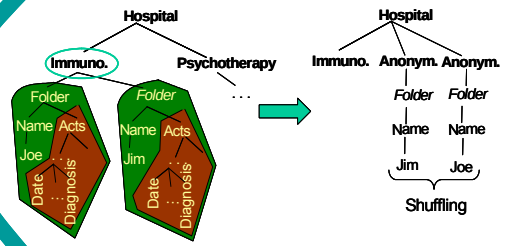


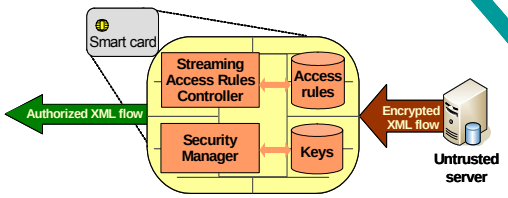
1 - Or-BAC, AdOr-BAC

- **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**



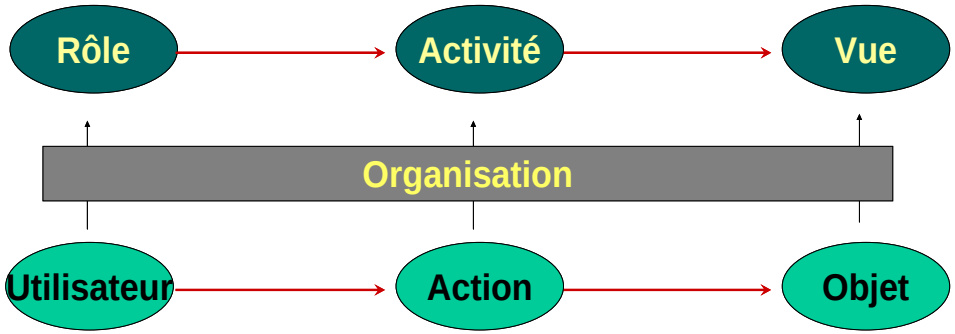


3 - Sécurisation du Contrôle

- **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

ACI Sécurité Informatique
C.A.S.C (2003-2006)

Contact : Luc Bouganim
E-mail : Luc.Bouganim@inria.fr
http://www-smis.inria.fr/~bouganim/CASC/

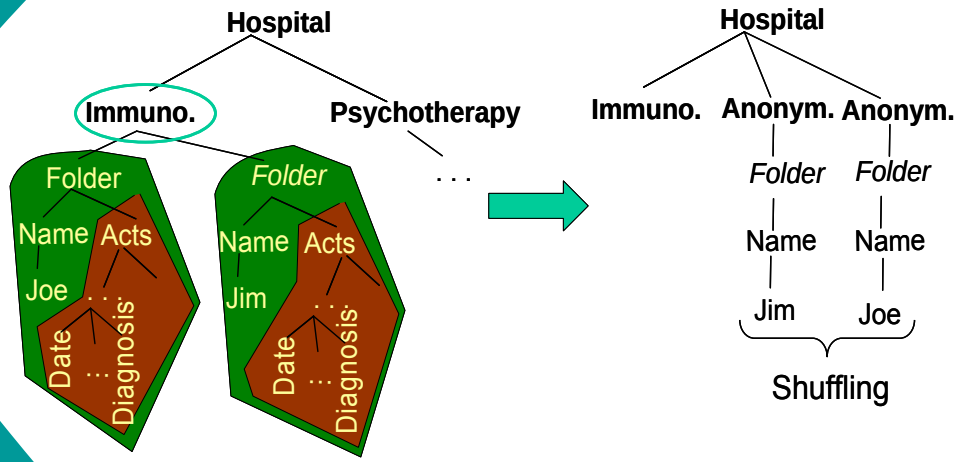


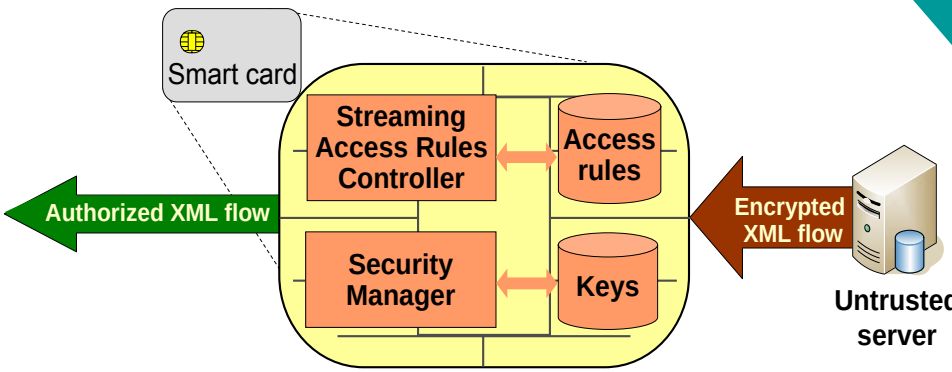
1 - Or-BAC, AdOr-BAC

- **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**



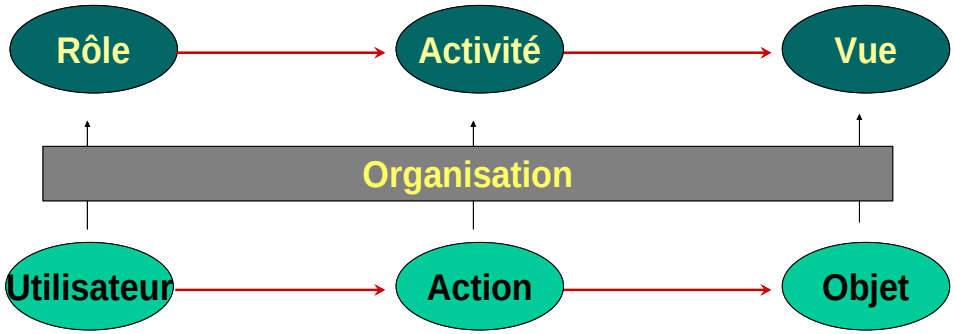


3 - Sécurisation du Contrôle

- **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

ACI Sécurité Informatique

C.A.S.C (2003-2006)

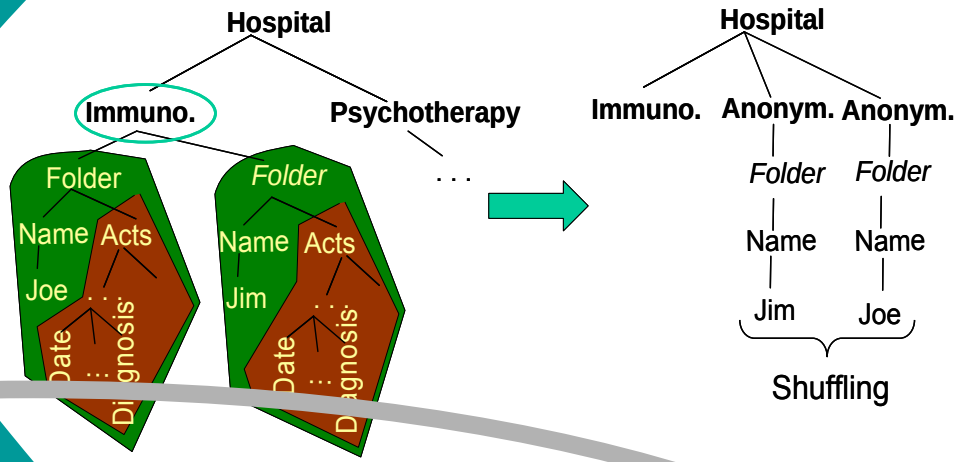


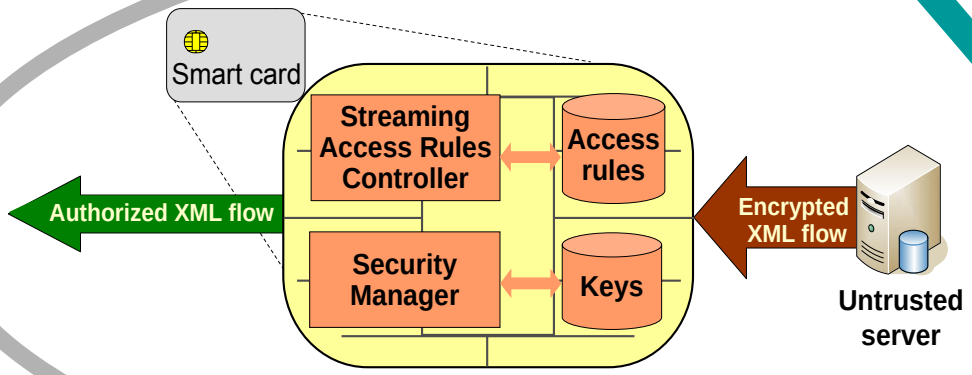
1 - Or-BAC, AdOr-BAC

- **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

ACI Sécurité Informatique

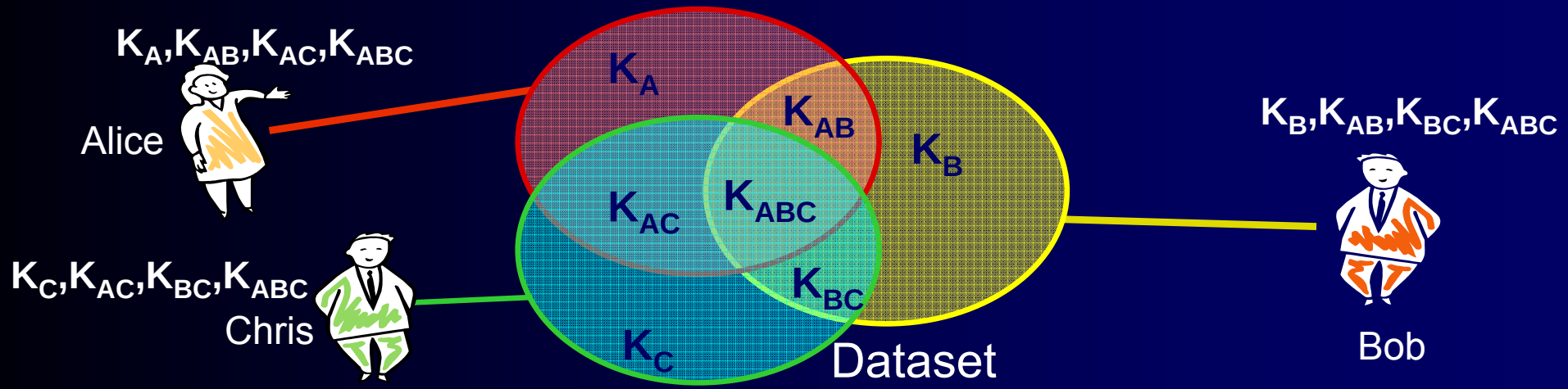
C.A.S.C (2003-2006)

Tamper-resistant access control management

- **Weaknesses of server-based access control**
  - External and Internal attacks
    - Erosion of trust put in database servers
  - Untrusted Database Service Providers (DSP)
  - Inadequate for some distribution channels
    - e.g., selective dissemination of data
- **Emergence of secured client devices**
  - e.g., Smart cards, secure tokens
- **Objectives**
  - Enforce the access control at the client side
  - Focus on XML access control

Existing client-based approaches

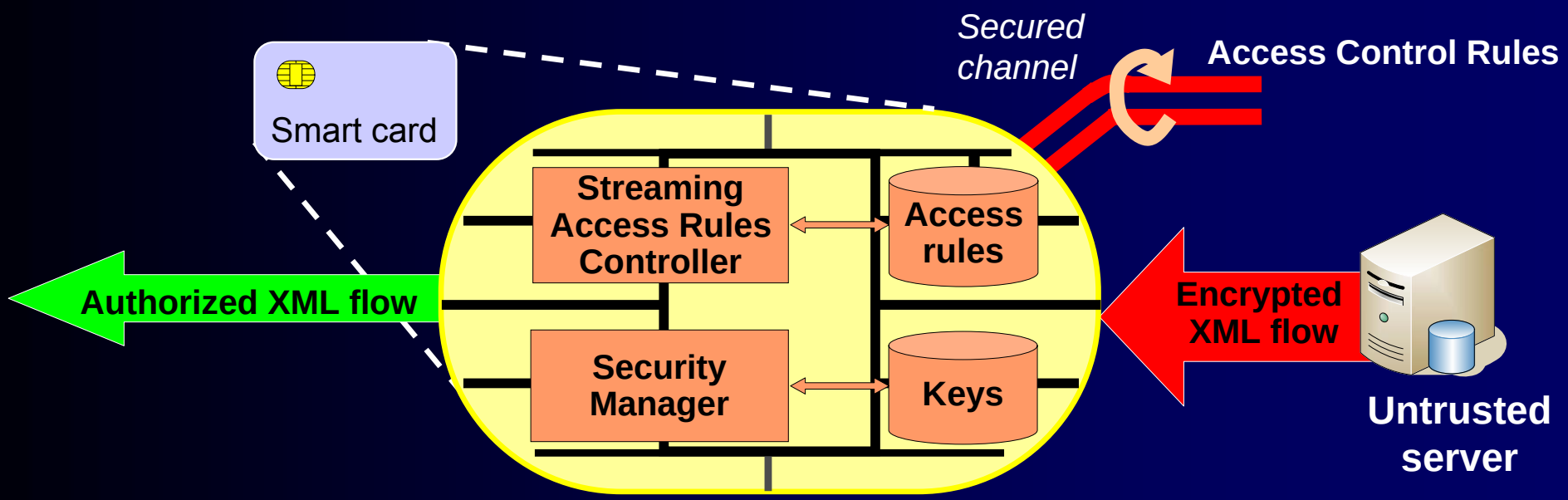
- **Traditional approaches**
  - Access rights enforced by means of encryption
  - Sharing depends on the decryption keys a client owns
- **Static and coarse-grain access control policies**
  - Right update ➔ re-encryption and key redistribution
  - Up to 2^n-1 keys for n user



Proposed approach

- **Access control evaluator embedded in a Trusted Computing Base (TCB)**
  - e.g., Smart cards, secure tokens
  - Incorruptible filtering element
  - re-establish the orthogonality between encryption and access control

  ➔ Dynamic and fine grain access control policies



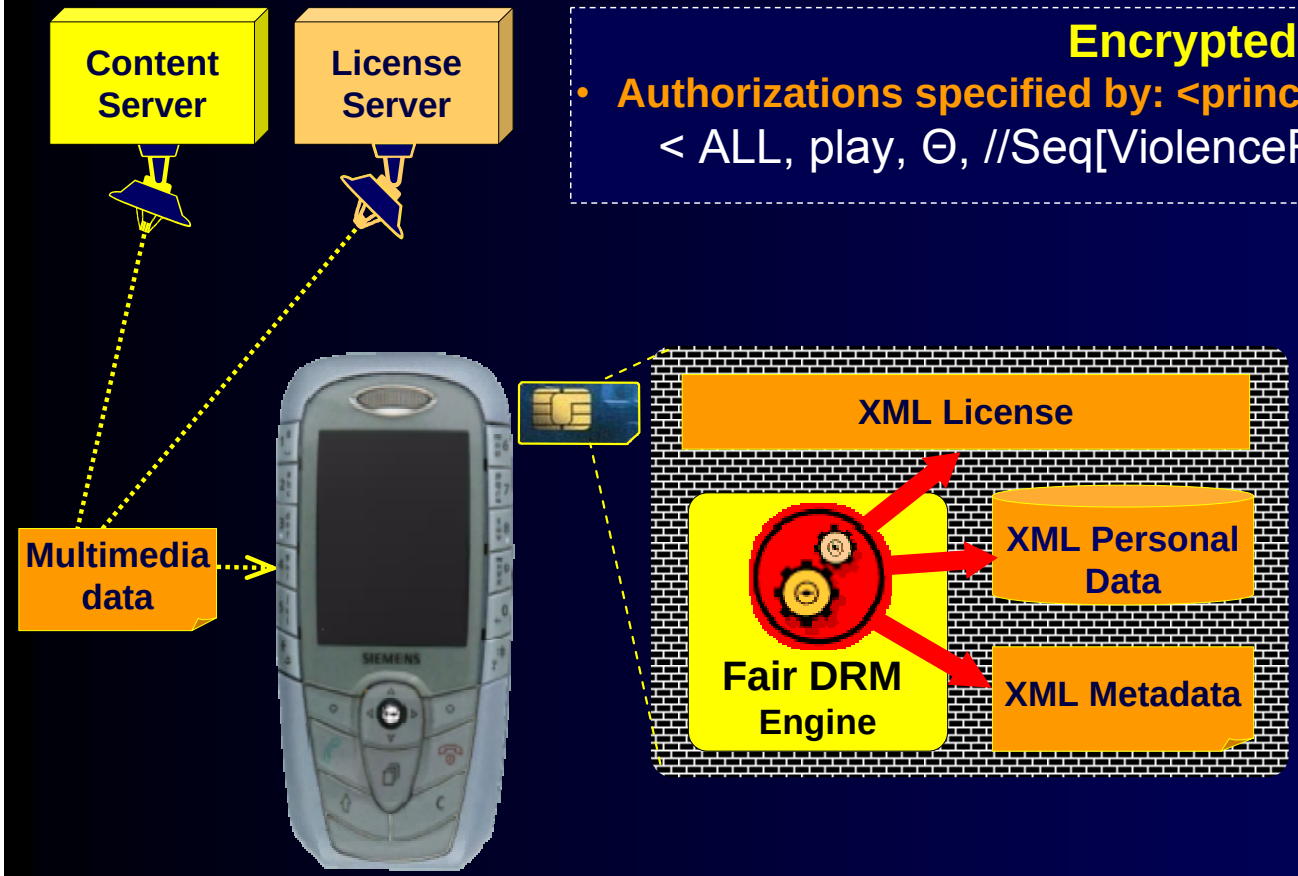
Problem Statement & contributions

- **Problems**
  - –TCB has a very small RAM memory precluding materialization
  - –Irrelevant data induces high communication and decryption costs
  - –Document tampering may mislead the access control
- **Contributions**
  - –Streaming access control based on non deterministic automata
  - –Streaming indexation to skip prohibited parts
  - –Tamper resistance f the XML stream enforced thanks to cryptographic techniques adapted to random accesses
- **Application to "Fair Digital Right Management"**

The case for Fair DRM

- **Why DRM ?**
  - Killer application for XML access control…
  - Our own challenge: Privacy and Fairness in DRM models
- **Definition of "Fair use"**
  - Limited free use of copyrighted material (1976 U.S. Copyright law)
  - **Broader sense:** to preserve the interest of each party (consumers, content providers, content distributors, etc.)
- **Providers' and distributors' point of view**
  - To have strong guarantees against large scale piracy
- **Consumer's point of view**
  - Possibility to share and loan what you paid for
  - To have strong privacy guarantees
- **Societal point of view**
  - Ethic enforcement: protect children against injuring content
  - Fair superdistribution: facilitate the access to valuable content for some categories of citizens: students, needy persons, artists, etc.

Application architecture



Encrypted XML Licenses

- **Authorizations specified by: <principal, action, sign, resource, condition(s)>**

< ALL, play, Θ, //Seq[ViolenceRating > /Profile/Violence]>

XML Personal Data

- **User profile**
- **Historical data**

Encrypted XML Metadata

- **XML Fine grain description of the multimedia data:**
  - Video Sequence description
  - Ratings (violence, sex, etc.)

a fair DRM virtual machine

Résultats – (1) Formalisation des modèles

- F. Cuppens, P. Pucheral, « Sécurité des bases de données », chapitre d'une encyclopédie informatique, Editions Vuibert, à paraître.
- F. Cuppens, A. Miège, 'Administration Model for Or-BAC' . International Federated Conferences (OTM'03), Workshop on Metadata for Security. Catania, Sicily, Italy, 2003.
- F. Cuppens F., A.Miège (2003). Modelling contexts in the Or-BAC model, 19th Annual Computer Security Applications Conference, Las Vegas, décembre 2003.
- F. Cuppens, A. Miège, 'Organization Based Access Control'. Druide, Le Croisic, 2004.
- F. Cuppens. Le modèle Or-BAC (Organization Based Access Control). Conférence invitée présentée au Premier Atelier Sécurité des Systèmes d'Information. Biarritz, France. Mai 2004.
- T. Sans et F. Cuppens. Vers une sémantique formelle pour les langages de DRM. Premier Atelier Sécurité des Systèmes d'Information. Biarritz, France. Mai 2004.
- F. Cuppens et A. Miège. Administration Model for Or-BAC. International Journal of Computer Systems Science and Engineering (CSSE), 2004.
- F. Cuppens, N. Cuppens-Boulahia, 'High level conflict management strategies in advanced access control models'. Rapport technique ENST Bretagne. Avril 2005.
- A. Gabillon. 'Multilevel Databases'. To appear in the Encyclopedia of Database Technologies and Applications (Mai-june2005)
- P. Pucheral, "Ubiquité et confidentialité des données", chapitre du livre « Paradigmes et enjeux de l'informatique» édité par le département STIC du CNRS, éditions Hermès, 2005.

Résultats – (2) Modèles de contrôle d'accès XML

- V. Benzaken, M. Burelle, G. Castagna, 'Information flow security for XML transformations'. In ASIAN 2003, Bombay, 2003.
- V.Benzaken, G.Castagna, C.Miachon, 'A Full Pattern-based Paradigm for XML Query Processing'. In the Seventh International Symposium on Practical Aspects of Declarative Languages PADL 2005, LNCS 3350 Springer-Verlag
- M. Bugliesi, G. Castagna, S. Crafa, R. Focardi, and V. Sassone. 'Name-passing calculi and crypto-primitives: a survey'. In Foundations of Security Analysis and Design, number 2946 in Lecture Notes in Computer Science, pages 91-138. Springer, 2004.
- B.Finance, S. Medjdoub, P. Pucheral, "Privacy of Medical Records: from Law Principles to Practice", Proc. of the 18th IEEE Int. Symp. on Computer-Based Medical Systems (CBMS), Dublin, Ireland, June 2005.
- B. Finance, S. Medjdoub, P. Pucheral, "The Case for Access Control on XML Relationships", ACM CIKM 2005.
- A. Gabillon and M. Fansi. A Persistent Labelling Scheme for XML and tree Databases. To be presented at IEEE SITIS 2005.
- A. Gabillon. A Formal Access Control Model for XML Databases. Proc. of the second VLDB Workshop on Secure Data Management. Trondheim, Norway. September 2005.
- A. Gabillon A Secure XML Database. SAR 2005. 4th Conference on Security and Network Architectures. June 06-10, 2005. Batz sur Mer France.
- M. Fansi. Prototype de Bases de Données XML sécurisée. Actes du 2eme atelier sur la Sécurité des Systèmes d'Information (SSI'05). Inforsid Grenoble. 24 mai 2005.
- A. Gabillon. An Authorisation Model for XML DataBases. Proc. of the 11th ACM Conference on Computer Security (Workshop Secure Web Services). George Mason University, Fairfax, VA, USA. October 2004
- A. Gabillon. Modèle de Contrôle d'Accès. Application à XML. INFORSID 2003. Nancy, Juin 2003
- F. Cuppens, N. Cuppens-Boulahia, T. Sans, Protection of relationships in XML documents with the XML-BB model, ICISS, 2005

Résultats – (3) Sécurisation du contrôle

- L. Bouganim, F. Dang Ngoc, P. Pucheral : ‘Client-Based Access Control Management for XML documents’. 30th International Conference on Very Large Data Bases, VLDB'04, Toronto, 2004.
- L. Bouganim, C. Cremarenco, F. Dang Ngoc, N. Dieu, P. Pucheral « Safe Data Sharing and Data Dissemination on Smart Devices » ACM SIGMOD 2005, demo session, Baltimore, USA, June 2005.
- L. Bouganim, N. Dieu, P. Pucheral, « MobiDiQ: Mobile Digital Quietude ». Gold Award of the SIMagine contest organized by Sun, Samsung and Axalto, 2005
- L. Bouganim, F. Dang Ngoc, P. Pucheral, « Chip-Secured XML Access ». Silver Award of the e-gate open 2004 contest organized by Sun, Axalto and STMicroelectronics, 2004.
- P. Pucheral, "A Data-Centric Approach of Smart Devices", International workshop on Construction and Analysis of Safe, Secure and Interoperable Smart devices (CASSIS), invited talk, March 2005.
- L. Bouganim, F. Dang Ngoc, P. Pucheral : ‘A Smart XML Access Right Controller for Mobile Applications’. e-Smart Conference, Sophia Antipolis, 2004.
- L. Bouganim, F. Dang Ngoc, P. Pucheral : ‘Sécurisation matérielle du contrôle d’accès à des documents XML’, Revue Ingénierie des Systèmes d’Information (ISI), n° spécial des meilleurs articles de BDA’04.
- L. Bouganim, F. Dang Ngoc, P. Pucheral : ‘Tamper-Resistant Ubiquitous Data Management’. International Journal of Computer Systems Science and Engineering (CSSE), Special Issue on Mobile Databases, 2005.

Merci !

Plus d’informations :

- **Luc.Bouganim@inria.fr**
- **http://www-smis.inria.fr/~bouganim/CASC**