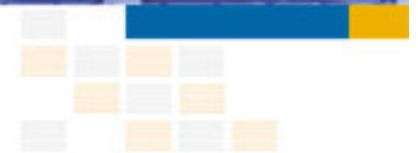


- École Nationale Supérieure
des Télécommunications de Bretagne



Le modèle Or-BAC

Organization Based Access Control

Nora Cuppens -Équipe SERES – ENST-Bretagne

www.enst-bretagne.fr

SEE 21 octobre 2004

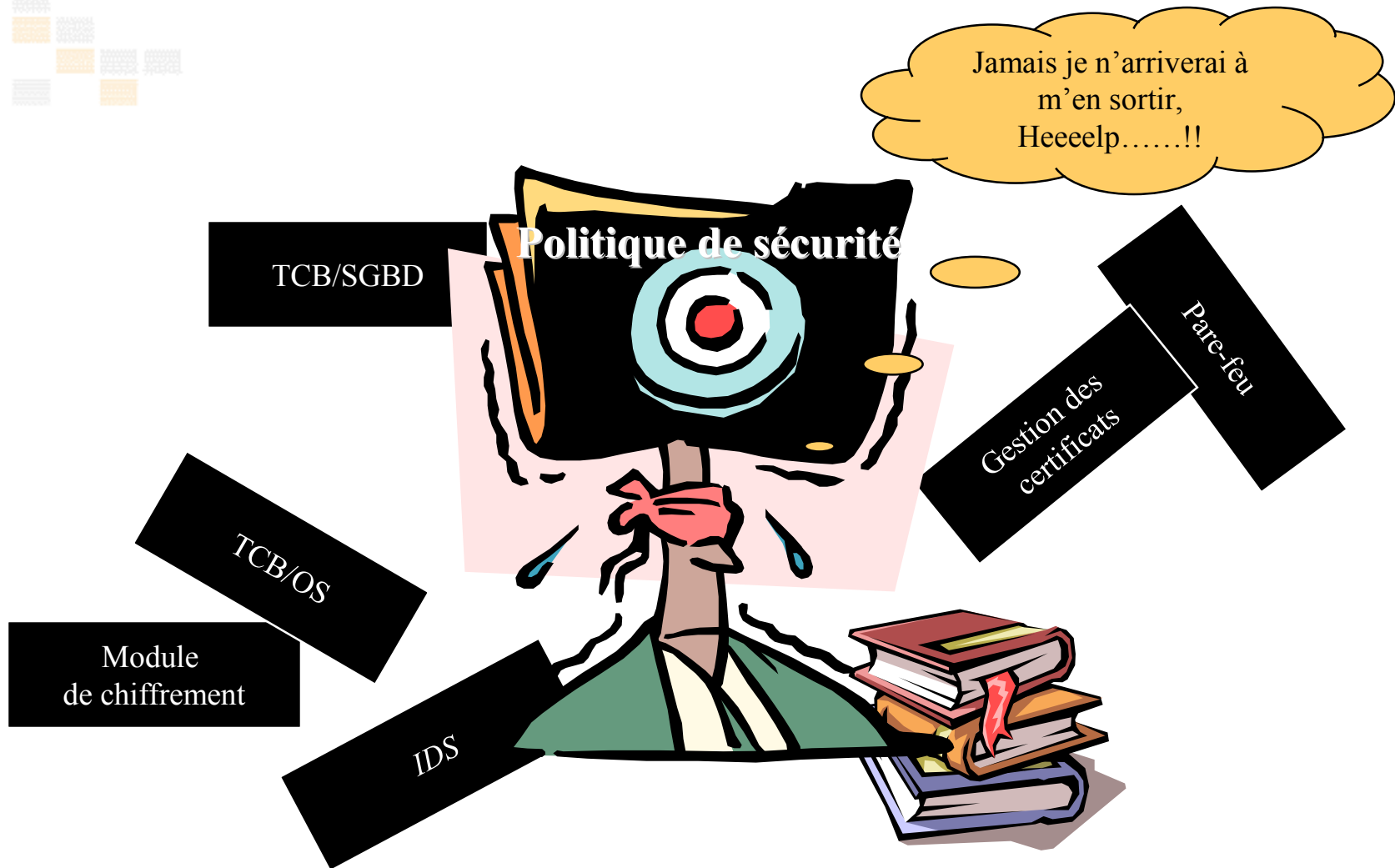


■ Plan

- Introduction
- Or-BAC et ses extensions
- Les entités du modèle
- Le contrôle d'accès Or-bac-isé
- Hiérarchie
- Gestion des conflits
- Administration
- Conclusion

Introduction :

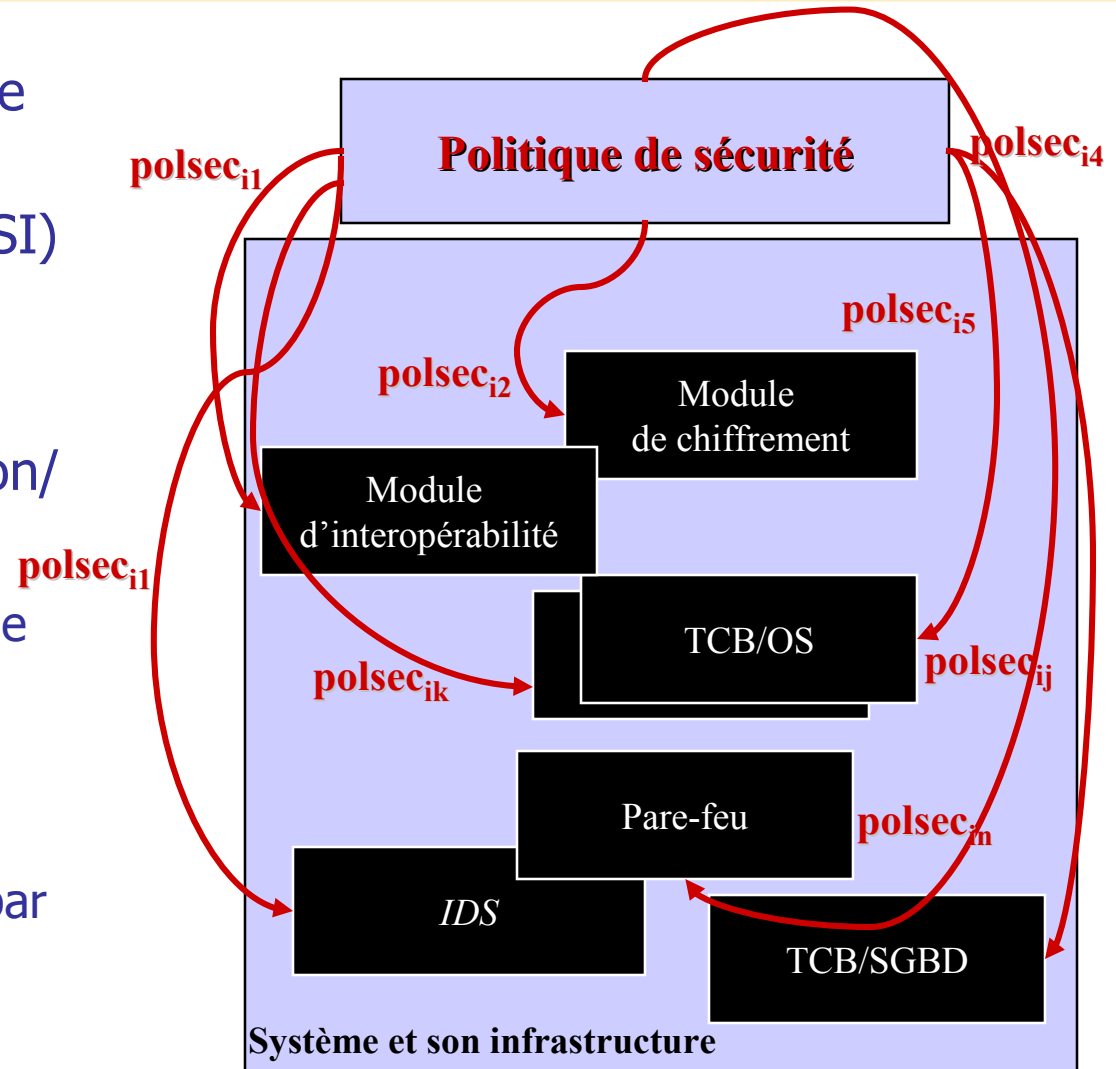
■ Définition et mise en œuvre d'une politique de sécurité



nora.cuppens@enst-bretagne.fr

■ Introduction : Une approche globale

- Définition de politiques de sécurité globales des systèmes d'information (SI)
- Processus de raffinement/décomposition/affectation
 - Configurer la politique de sécurité déléguée à chacun des composants d'une architecture de sécurité mise en place par les SI



nora.cuppens@enst-bretagne.fr

■ Introduction : Gestion locale des Polsec_{ij}

- Chaque composant de sécurité du SI possède sa propre politique qu'il doit gérer en conformité avec la politique de sécurité globale
- Chacune des ses politiques correspond à une politique de contrôle d'accès
- Objectif
 - modèle générique pour exprimer ces politiques de contrôle d'accès
 - lequel ?

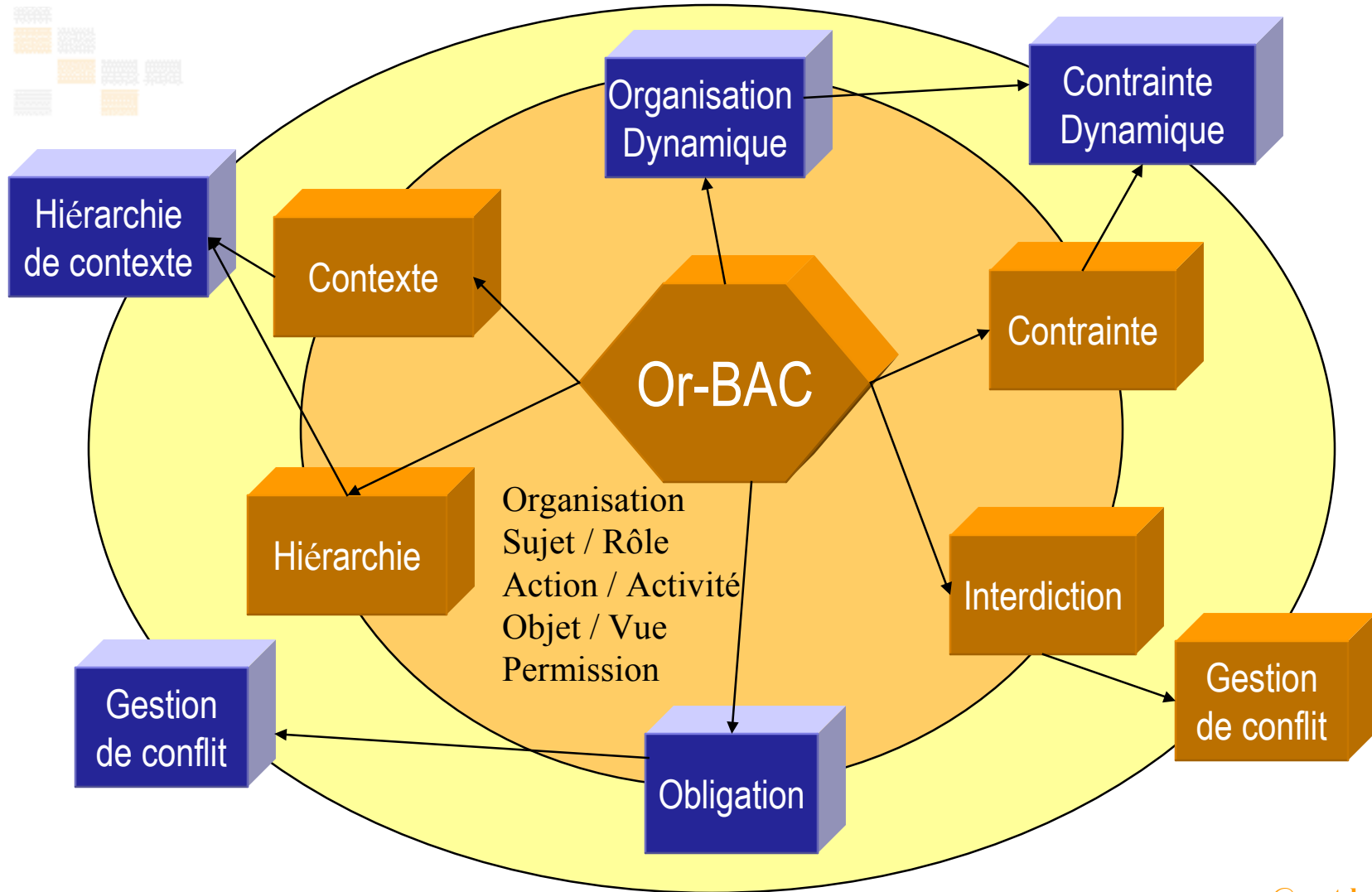
■ Introduction : politique d'autorisation

■ Le contrôle d'accès

- Exprimé par un ensemble d'autorisations
- Spécifié par des administrateurs de sécurité ou de simples utilisateurs
- Conformément à une certaine politique de sécurité
- Approche conventionnelle (sujet, objet, privilège)
 - Insuffisante pour répondre aux nouveaux systèmes et aux nouvelles applications
 - Manque d'expressivité
 - Interdiction, rôle, tâche, contenu, contexte, ...
- Résultat : une grande variété de modèles
 - Différences : composants, expressivité et administration
 - ... et Or-BAC

nora.cuppens@enst-bretagne.fr

Or-BAC et ses extensions



nora.cuppens@enst-bretagne.fr

■ Le modèle Or-BAC : *cœur du modèle*

- L'organisation est l'entité centrale du modèle
- Pourquoi cette structuration ?
 - Décliner une politique de sécurité suivant les organisations
 - Formalisme commun
 - Assurer l'interopérabilité de différentes organisations
 - Hiérarchiser l'organisation
 - Décomposer la politique de contrôle d'accès dans les sous organisations (départements, unités, ..., composants de sécurité réseau)

■ Le modèle Or-BAC : *entités du modèle*

■ Les rôles

- Concept introduit dans le modèle RBAC

→ Un *sujet* obtient des permissions en fonction du ou des rôles qu'il joue *dans une certaine organisation*

→ Ex : Jean joue le rôle de responsable technique du CESTI Rêve

■ Les activités

- Abstraction des *actions*

→ Vision classique des actions

→ Interaction entre les sujets et les objets (lire, écrire, ...)

- Une activité est un ensemble d'actions ayant des propriétés communes

■ Les vues

- Abstraction des *objets*

→ Entité passive au sens traditionnel

- Proche du concept de vue dans les bases de données

nora.cuppens@enst-bretagne.fr

■ Le modèle Or-BAC : *entités du modèle*

■ Les contextes

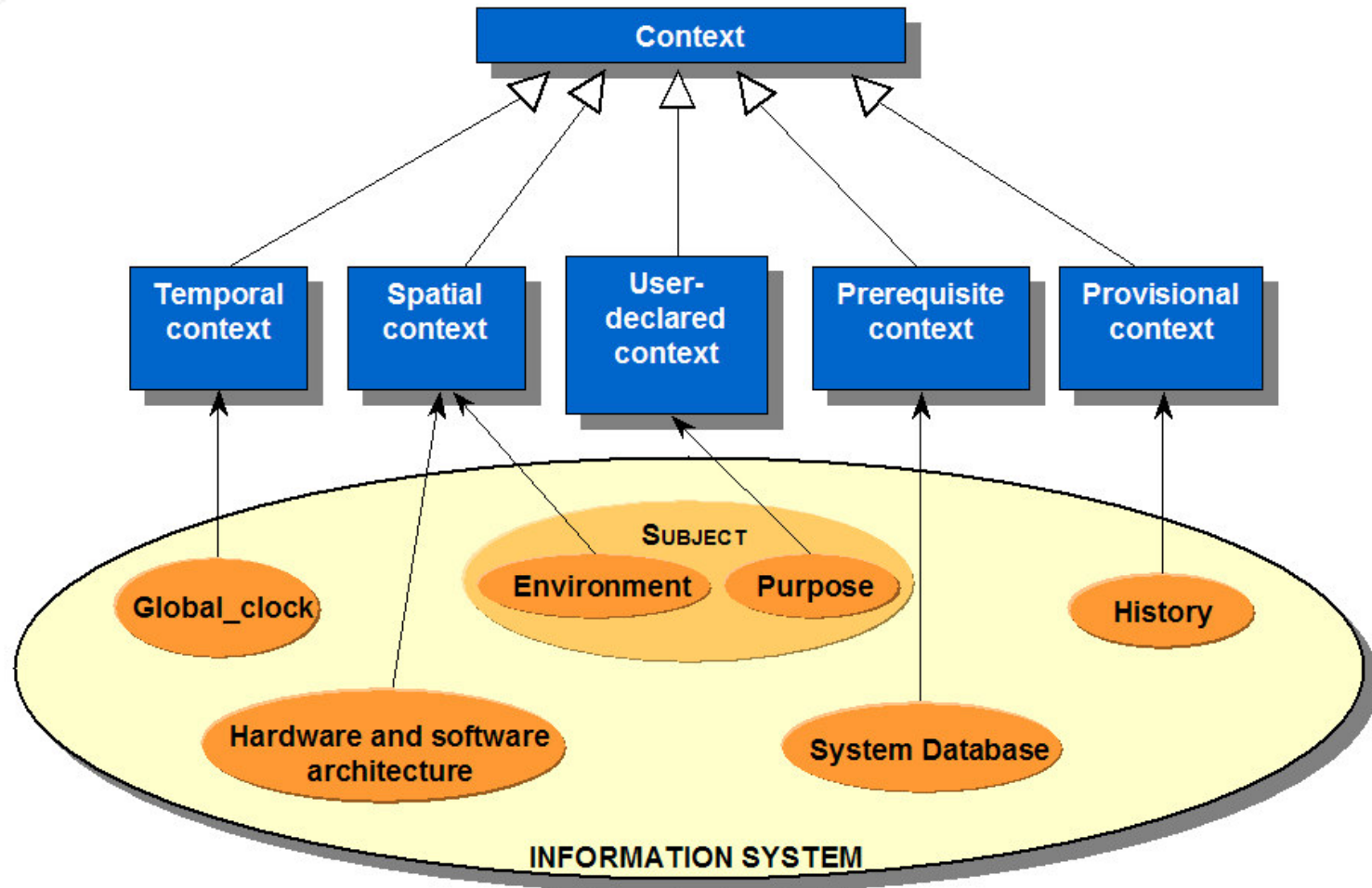
- Abstraction de **contraintes** à respecter pour l'attribution des privilèges
 - Temporel : l'heure de la journée
 - Environnemental : l'état du système (mode normal, mode dégradé)
 - Spatial : lieu d'exécution de l'activité
 - Provisionnel : activités préalablement réalisées



Une taxinomie de contextes

Le modèle Or-BAC : *entités du modèle*

Taxinomie de contextes*



*ACSAC 2003

nora.cuppens@enst-bretagne.fr

■ Le modèle Or-BAC : *entités du modèle*

■ Exemples de contextes

■ Contexte défaut

Organisation(org) \wedge Sujet(s) \wedge Action(a) \wedge Objet(o)
→ Hold (org, s, a, o, défaut)

■ Contexte *heure_de_travail*

Sujet(s) \wedge Objet(o) \wedge Action(a)
08:00 \leq GLOBAL_CLOCK \wedge GLOBAL_CLOCK \leq 19:00
→ Hold (ENST-Bretagne, s, a, o, heure_de_travail)

■ Contexte propriétaire

use(system-gest-fichier,o,home-repertoire) \wedge Owner(o,s) \wedge Action(a)
→ hold(system-gest-fichier,s,o,a,proprietaire)

■ *Context calculus*

- Contexte conjonctif, disjonctif, négatif
- *propriétaire & heure_de_travail*

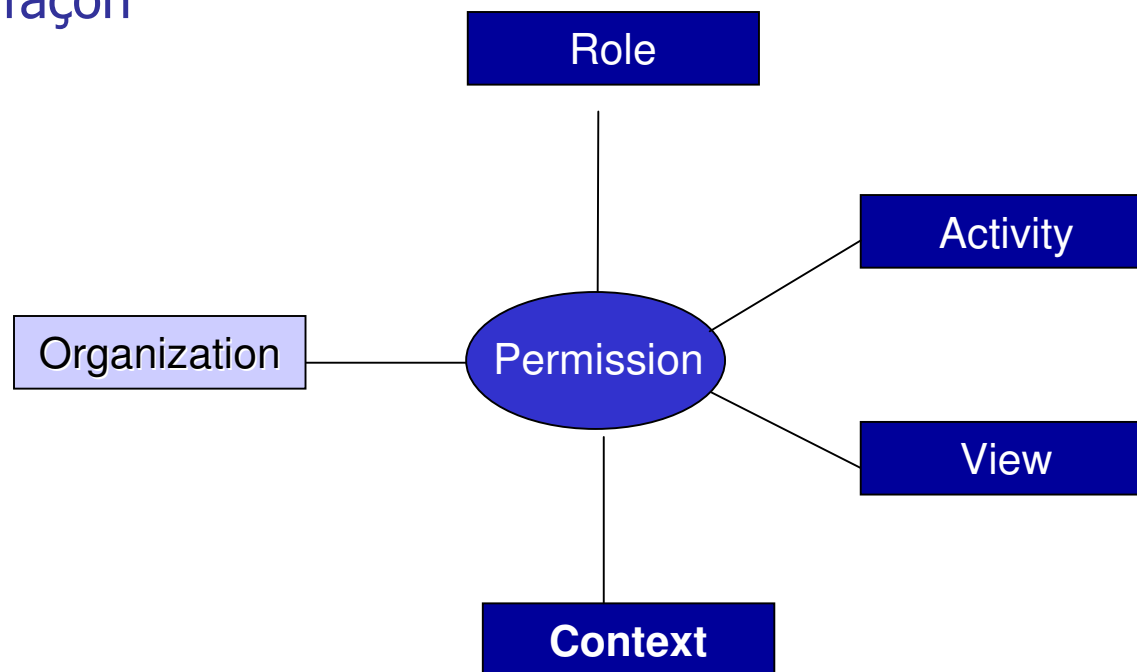
nora.cuppens@enst-bretagne.fr

■ Définition d'une politique de contrôle d'accès

■ Introduction des *Permissions*

■ *Permission (Organization, Role, Activity, View, Context)*

→ Les interdictions et les obligations sont définis de la même façon



nora.cuppens@enst-bretagne.fr

■ Dérivation du triplet passif [*sujet,action,objet*]

- Les permissions concrètes sont déduites des permissions abstraites

Règle GR1 :

Permission (org, role, activity, view, context) ∧
Empower (org, subject, role) ∧
Consider (org, action, activity) ∧
Use (org, object, view) ∧
Hold(org,subject,action,object,context) ∧
→ Is_permitted (subject, action, object)

■ Exemple de dérivation

■ `Permission(EnstBretagne,professeur,preparerCours,supportDeCours,
heure_de_travail) ^`

`Empower(Enst-Bretagne,Xavier,professeur) ^`

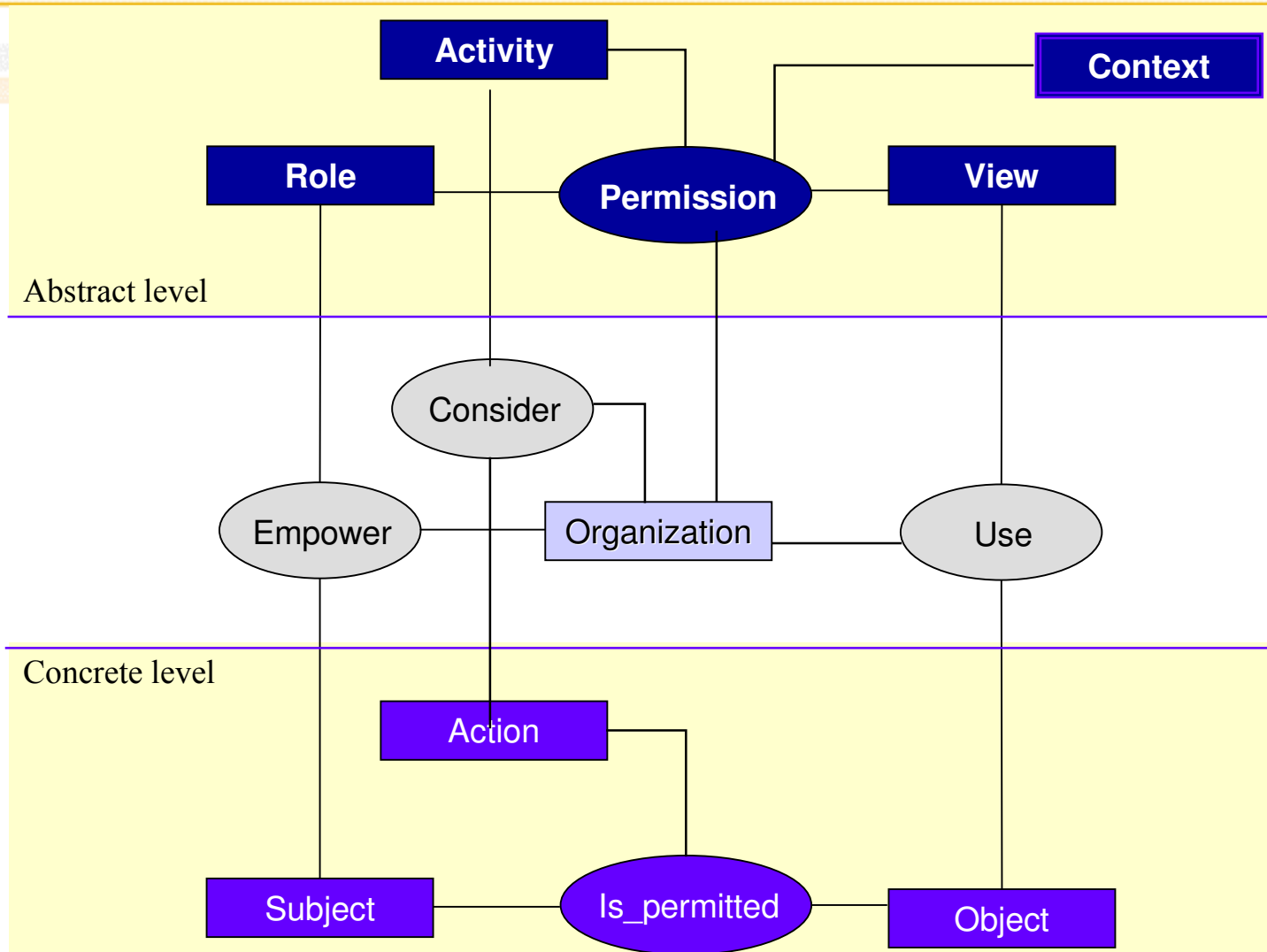
`Consider(Enst-Bretagne,latex,preparerCours) ^`

`Use(Enst-Bretagne,coursSecurite.tex,supportDeCours) ^`

`GLOBAL_CLOCK = 10:40`

→ `Is-Permitted(Xavier,latex,coursSecurite.tex)`

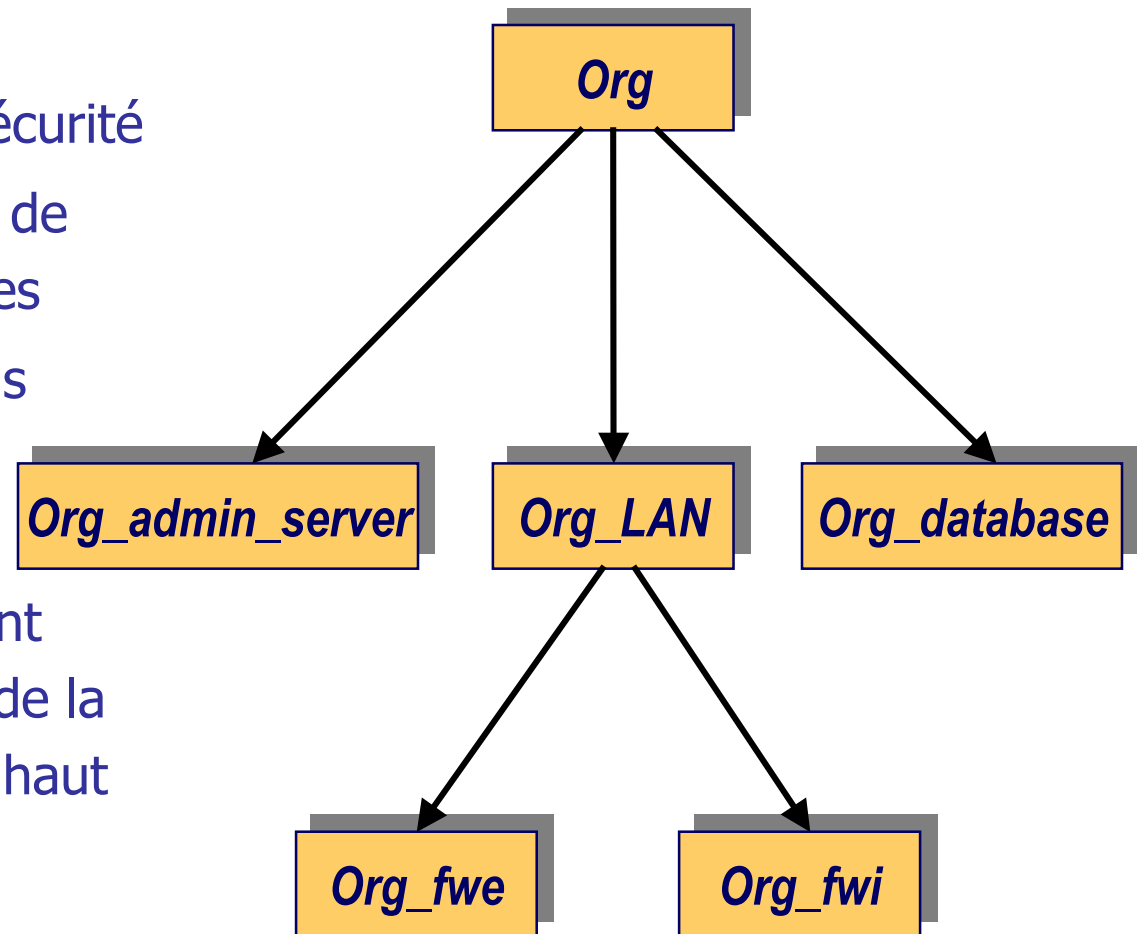
■ Contrôle d'accès Or-bac-isé



nora.cuppens@enst-bretagne.fr

■ Hiérarchisation/décomposition

- Allègement de la tâche d'administration de la sécurité
- Automatisation *partielle* de l'attribution des privilèges
- Définition d'un processus d'héritage *contrôlé* des privilèges
- Guide pour le raffinement et/ou la décomposition de la politique de sécurité de haut niveau



■ Politique de contrôle d'accès et conflits

■ Politique *ouverte*

- Tout ce qui n'est pas explicitement interdit est permis

■ Politique *fermée*

- Tout ce qui n'est pas explicitement permis est interdit

■ Politique *mixte* et gestion des exceptions

- Autorisations non conflictuelles
- Gestion des conflits entre permissions et interdictions
- Niveaux de priorité associés aux permissions et interdictions
- Résolution effectuée au niveau abstrait

■ Gestion des conflits

■ Définition

$$\text{Conflit} \leftrightarrow \text{Is_permitted}(s,a,o) \wedge \text{Is_prohibited}(s,a,o)$$

■ Exemple

*Is_permitted (Jean, acroread, fiche_client_33.pdf) et
Is_prohibited (Jean, acroread, fiche_client_33.pdf)*

■ Objectif

- Résoudre les conflits entre permissions et interdictions
- Respecter les contraintes
- Résolution au niveau abstrait

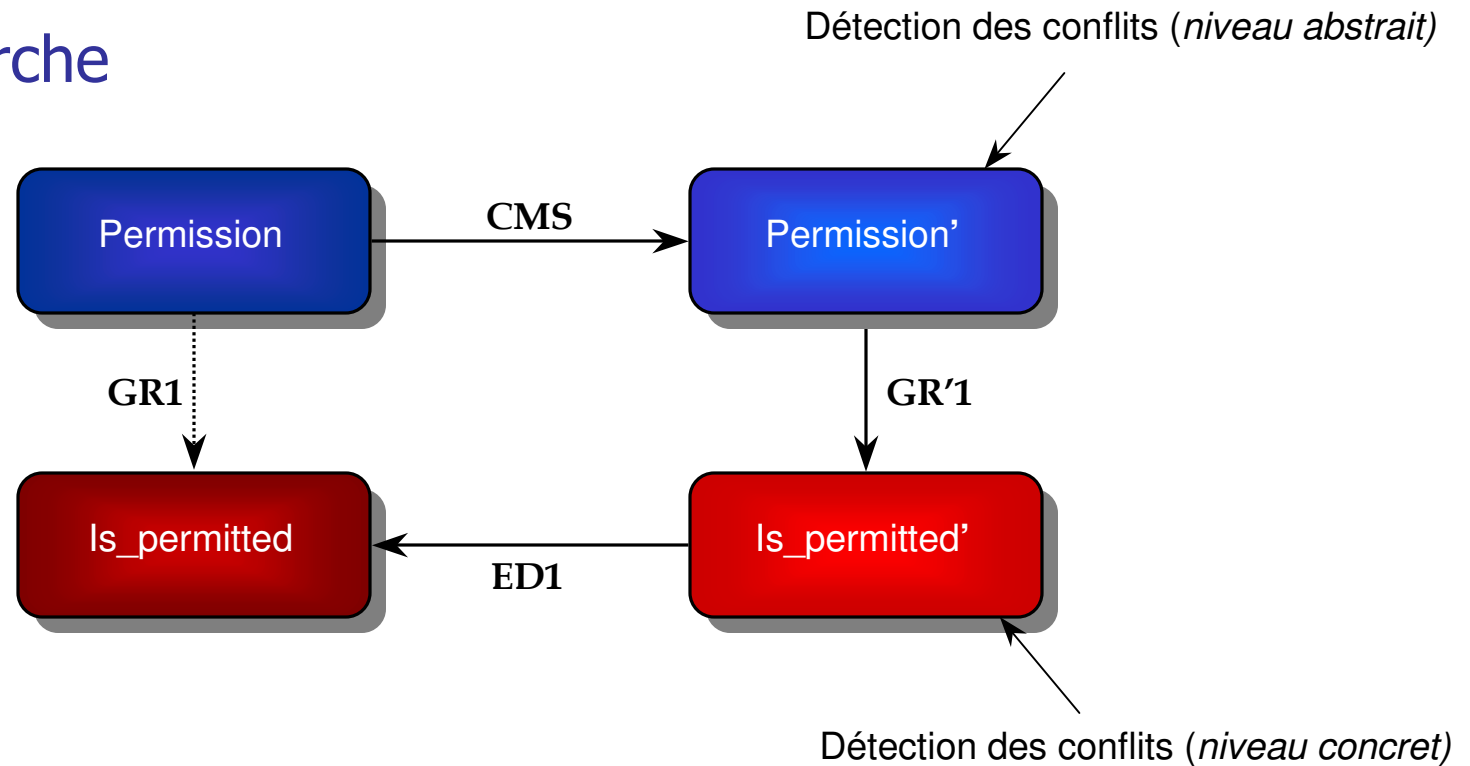
■ Principe

- Niveaux de priorité associés aux permissions et interdictions abstraites
- Définition d'une condition suffisante au niveau abstrait
 - ➔ Cette condition suffisante garantit, si elle est satisfaite, qu'aucun conflit ne pourra apparaître au niveau concret

nora.cuppens@enst-bretagne.fr

■ Gestion des conflits

■ Démarche



- *CMS : Stratégie de gestion des conflits*
 - *Introduction de priorités*
- *ED : Explicit Derivation*

■ Administration du modèle : AdOr-BAC*

- Principe : déterminer les droits correspondant à la réalisation des tâches administratives
 - Contrôler l'accès aux actions d'administration
- Objectifs
 - Absence de séparation entre les rôles administratifs et les rôles standard
 - Les règles administratives doivent avoir le même format que les règles standard
 - Possibilité de délégation
- Administration par la gestion de vues
 - URA, PRA et
 - UPA (délégation)

*(OTM'03)

nora.cuppens@enst-bretagne.fr

■ Administration du modèle

- Affectation des permissions aux rôles
 - *Vue PRA : Permission Role Assignment*

- Principe

- Donner une permission revient à créer un ticket

Billet d'avion

Compagnie aérienne	Numéro de vol
Nom du passager	Date et heure
	Numéro de siège

- Donner une permission = insérer un objet dans la vue PRA
 - Administrer les droits = définir les permissions sur PRA

nora.cuppens@enst-bretagne.fr

■ Conclusion

- Or-BAC répond aux exigences de complétude, de cohérence et de facilité attendu d'un modèle de contrôle d'accès
 - Structuration
 - Expressivité
 - Interface graphique
 - ➔ OtoKit pour la saisie, la vérification et la simulation d'une politique de sécurité
 - Résolution de conflits : mise en œuvre dans OtoKit
 - Administration
 - ➔ AdOr-BAC
 - Indépendance du niveau d'abstraction
 - ➔ Génération automatique de règles de configuration d'un pare-feu
- Spécification distribuée d'une politique de sécurité et interopérabilité

nora.cuppens@enst-bretagne.fr