École Nationale Supérieure
des Télécommunications de Bretagne

ENST Bretagne

Héritage de privilèges dans le modèle Or-BAC

Application dans un environnement réseau

Frédéric Cuppens, Nora Cuppens-Boulahia et Alexandre Miège

www.enst-bretagne.fr

SSTIC 02-04 juin 2004

get

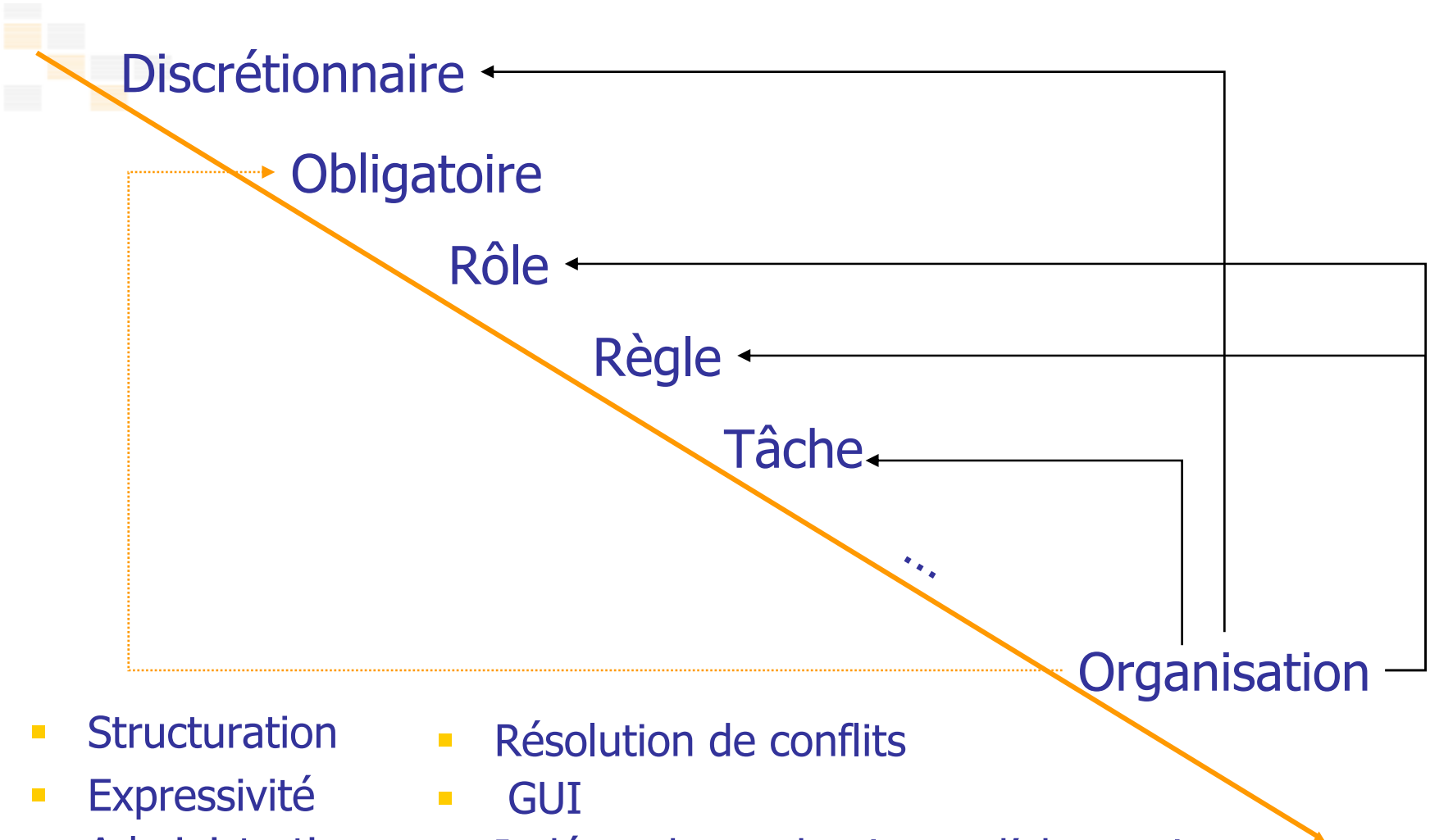
Plan

- Introduction
- Or-BAC dans la famille des modèles de contrôle d'accès
- Définition d'une politique de sécurité réseau
- Hiérarchiser l'organisation
  - Héritage des hiérarchies et des privilèges *(a)*
  - Concept de *pertinence* d'une entité Or-BAC dans une organisation *(b)*
- Spécifier des hiérarchies dans une organisation
  - Types de hiérarchies *(c)*
  - Affectation/dérivation des privilèges souhaités *(a)(b)(c)*
- Conclusion

Introduction

- Le contrôle d'accès
  - Exprimé à travers 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

Or-BAC dans la famille des modèles de contrôle d'accès



- Structuration
- Expressivité
- Administration
- Résolution de conflits
- GUI
- Indépendance du niveau d'abstraction

nora.cuppens@enst-bretagne.fr

Le modèle Or-BAC : *profil du modèle*

- Or-BAC : contrôle d'accès basé sur les organisations
- Objectif
  - Introduire un niveau d'abstraction permettant d'exprimer la politique de contrôle d'accès indépendamment de son implémentation
- Principes
  - Structuration via l'entité organisation
  - Deux niveaux d'abstraction
    - → Niveau concret : sujet , action , objet
    - → Niveau abstrait : rôle, activité , vue
  - Expression de permissions, d'interdictions et d'obligations
  - Expression de contextes

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 *médecin* à l'hôpital Sud
- 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

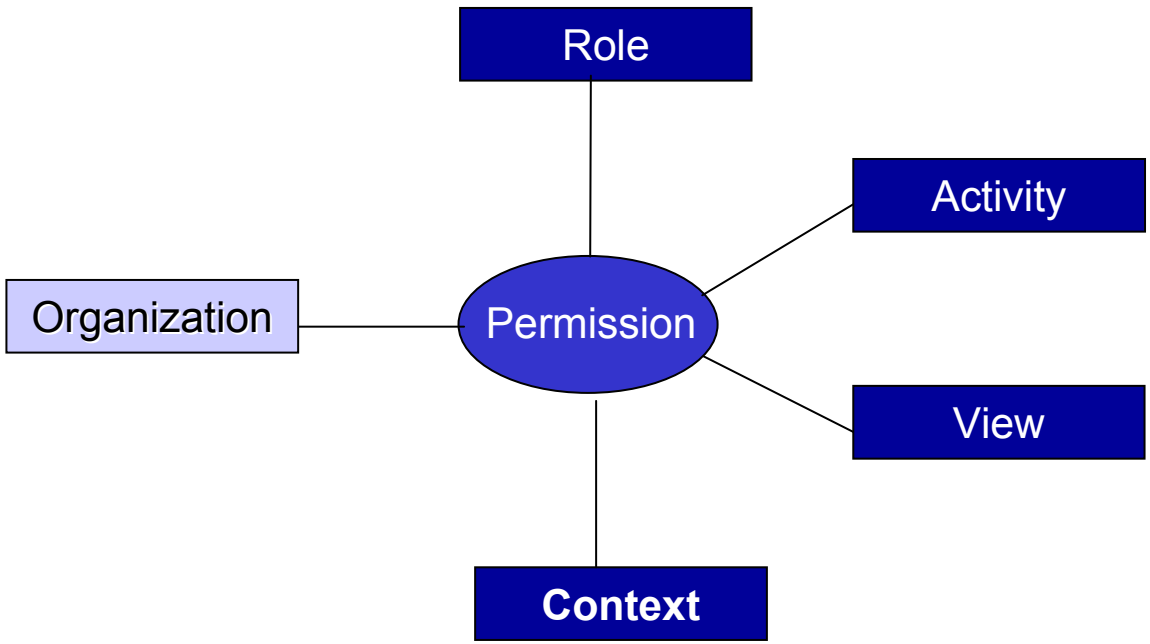
nora.cuppens@enst-bretagne.fr

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
    - …

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

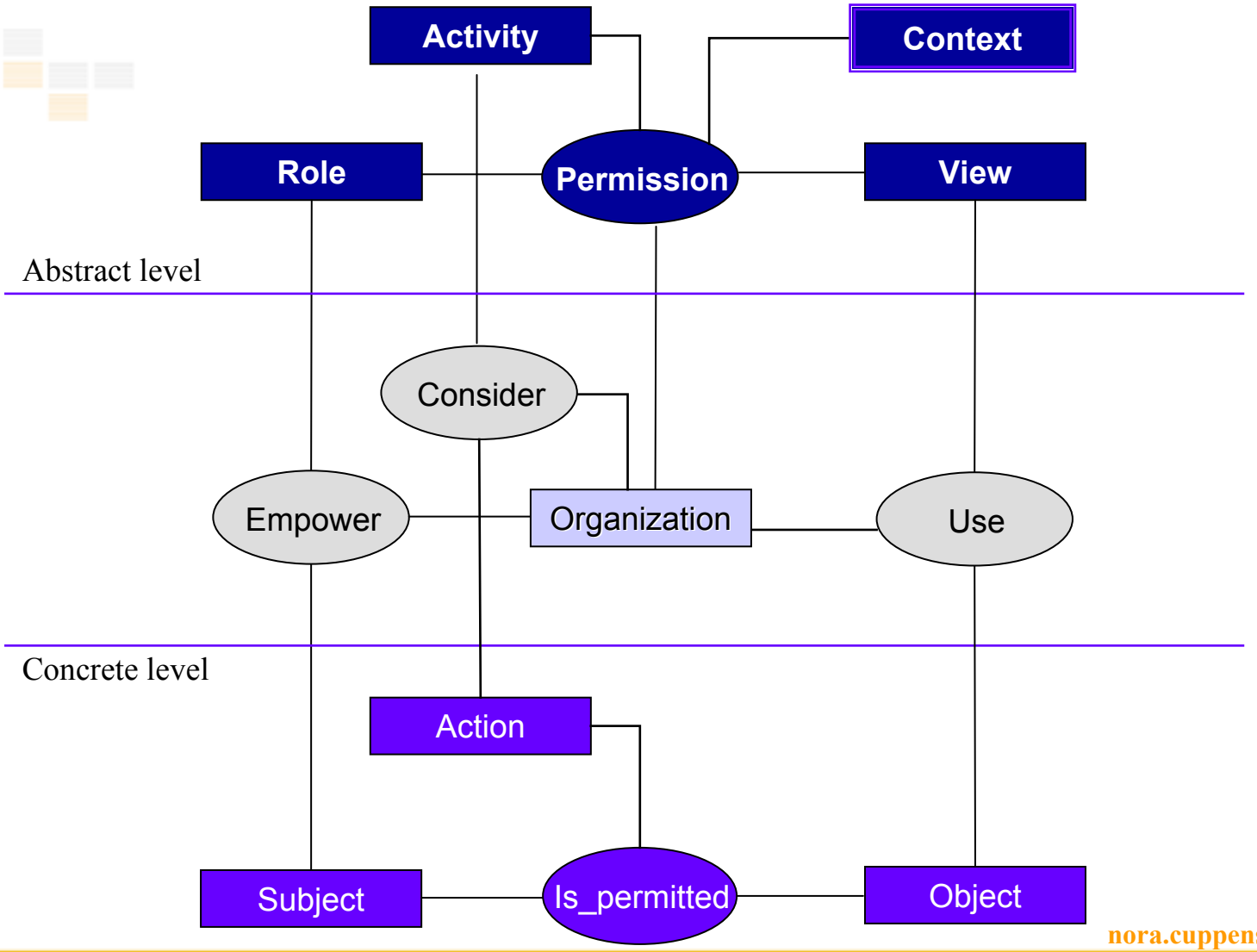


Définition d'une politique de contrôle d'accès

- Les permissions concrètes sont déduites des permissions abstraites
  - Règle RG1

$$\textbf{\textit{Permission}}\ (\textbf{\textit{org, role, activity, view, context}}) \wedge$$
$$\textit{Empower}\ (\textit{org, subject, role}) \wedge$$
$$\textit{Consider}\ (\textit{org, action, activity}) \wedge$$
$$\textit{Use}\ (\textit{org, object, view}) \wedge$$
$$\textit{Hold(org,subject,action,object,context)} \wedge$$
$$\rightarrow \textbf{\textit{Is\_permitted}}\ (\textbf{\textit{subject, action, object}})$$

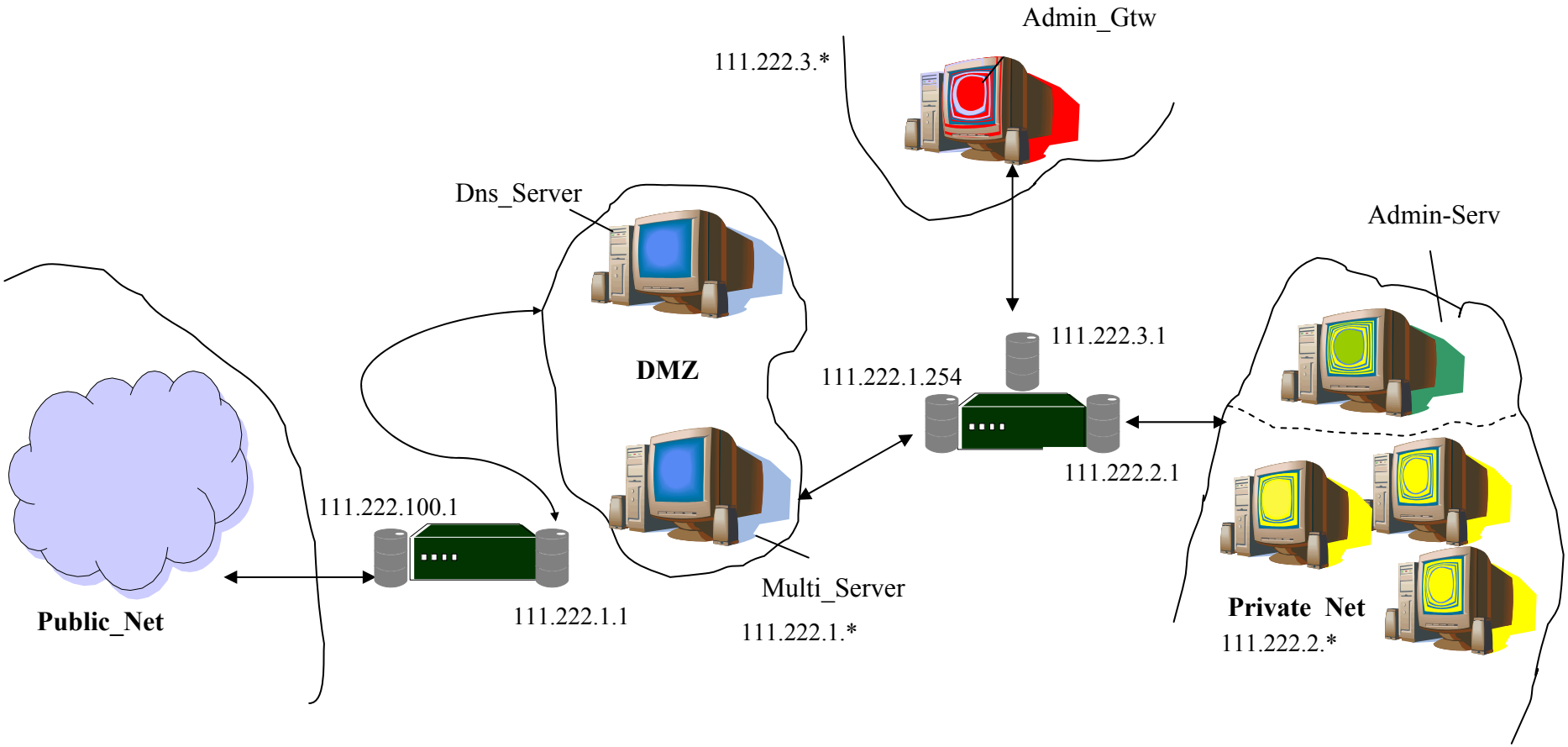
Contrôle d'accès Or-bac-*isé*



nora.cuppens@enst-bretagne.fr

Définition d'une politique de sécurité réseau

Application



Énoncé de la politique de sécurité réseau

- Les hôtes privés de Org peuvent accéder à Internet
- Les hôtes externes Public_net ne peuvent accéder qu'aux serveurs de la DMZ
- Les hôtes affectés au rôle de gestion des serveurs peuvent mettre à jour les serveurs de la DMZ
- Les interfaces des firewalls ne sont accessibles que par les hôtes affectés au rôle de gestion des firewalls
- …

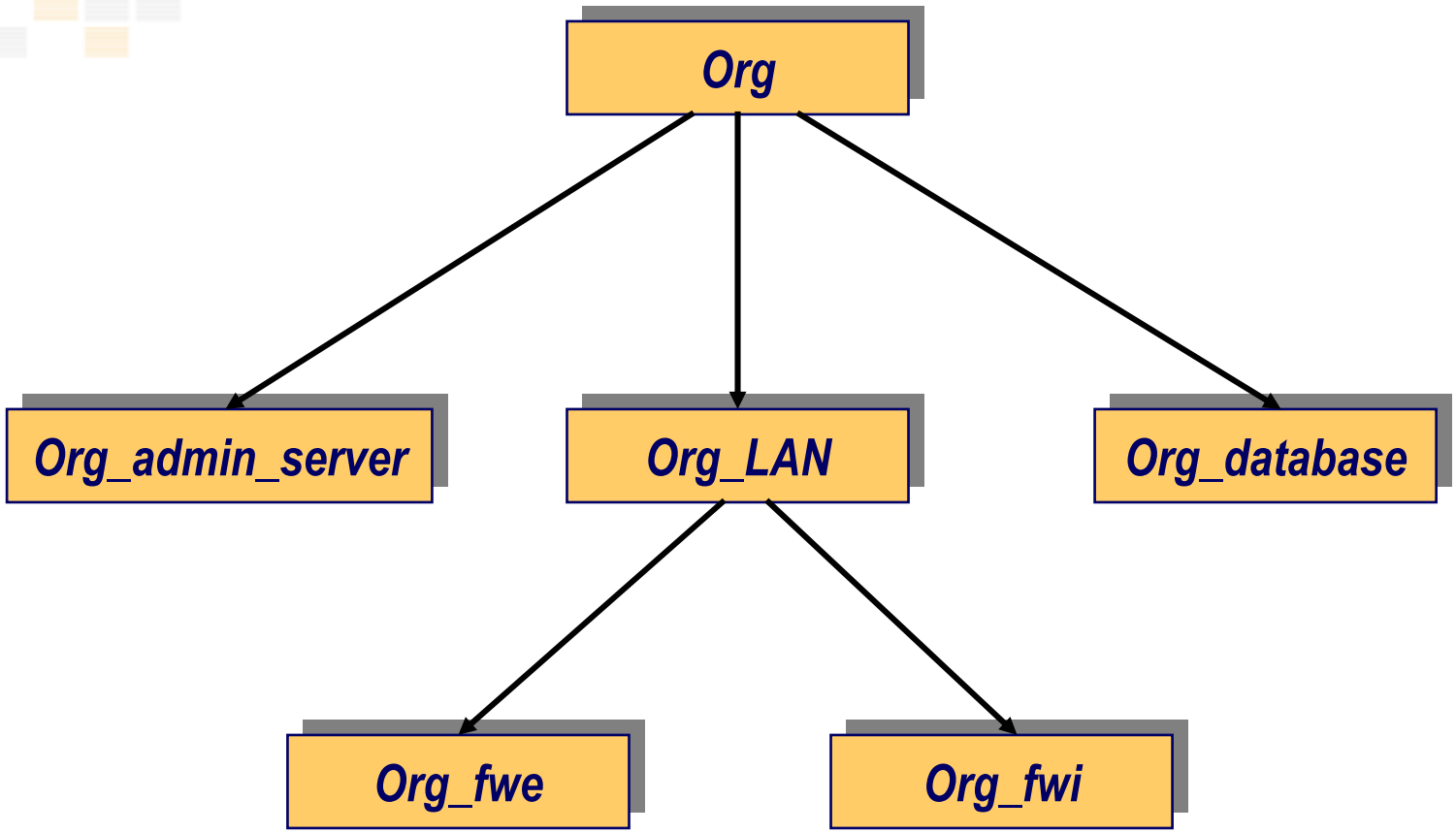
Objectifs

- Spécifier les permissions définissant cette politique de sécurité en utilisant Or-BAC
- Décomposer cette politique pour obtenir la politique de sécurité des deux firewalls
- Traduire les politiques pour générer les règles de configuration des deux firewalls

Hiérarchiser l'organisation « Org »

- Comment ?
  - Localiser les entités en charge de gérer des règles de sécurité
  - Dépend de la politique de sécurité à mettre en place
- Une hiérarchie possible,
  - L'organisation *Org (une banque, une entreprise, un hôpital,…)*
    - ➔ Le réseau local de l'organisation *Org_LAN*
      - La passerelle externe *Org_fwe* : le firewall1
      - La passerelle interne *Org_fwi* : le firewall2
    - ➔ Le serveur de base de données *Org_database*
    - ➔ L'administration des passerelles *Org_admin_fw*
- Une autre organisation dont il faut tenir compte mais vue par *Org* comme un rôle
    - ➔ Internet *Public_net* : réseau public

Hiérarchie d'organisations dans Org



nora.cuppens@enst-bretagne.fr

Les sujets

- Sujet = machine hôte
- Vue Host
- Chaque hôte a une adresse IP
  - Attribut : *address(h,a)*
    - ➔ L'adresse IP du hôte *h* est égale à *a*
- Zone ou groupe = sous-vue de Host
  - $Use(Org\_LAN,h,DMZ) \leftarrow$
    $Use(Org\_LAN,h,Host) \wedge address(h,a) \wedge a \in 111.222.1.*$

Définir des rôles : *exemples de rôles*

- *Public_host* : rôle pouvant être joué par un hôte de la zone public
- *Private_host* : rôle pouvant être joué par un hôte de la partie privée du réseau de l'organisation hors zones d'administration
- *Int_firwall* : rôle pouvant être joué par les interfaces du firewall frontal
- *Web_serveur* : rôle joué par le serveur de web
- *Adm_fw_host* : rôle joué par les hôtes d'administration des passerelles.

Fixer la pertinence rôles/organisations (1)

- Les rôles définis dans l'organisation *Org* n'ont pas forcément un sens pour toutes les sous-organisations de *Org*
- Exemple : le rôle « conseiller financier » dans une banque B
  - Il est défini dans l'organisation *B*
  - Il est défini dans la sous-organisation *Private_net_clientèle* de *Org_private_net* (Ex : guichetier, responsable_clientèle)
  - Il ne l'est pas dans la sous_organisation *Private_net_employé_sg de Org_private_net* (Ex : vigile, technicien de surface)

Fixer la pertinence rôles/organisations (2)

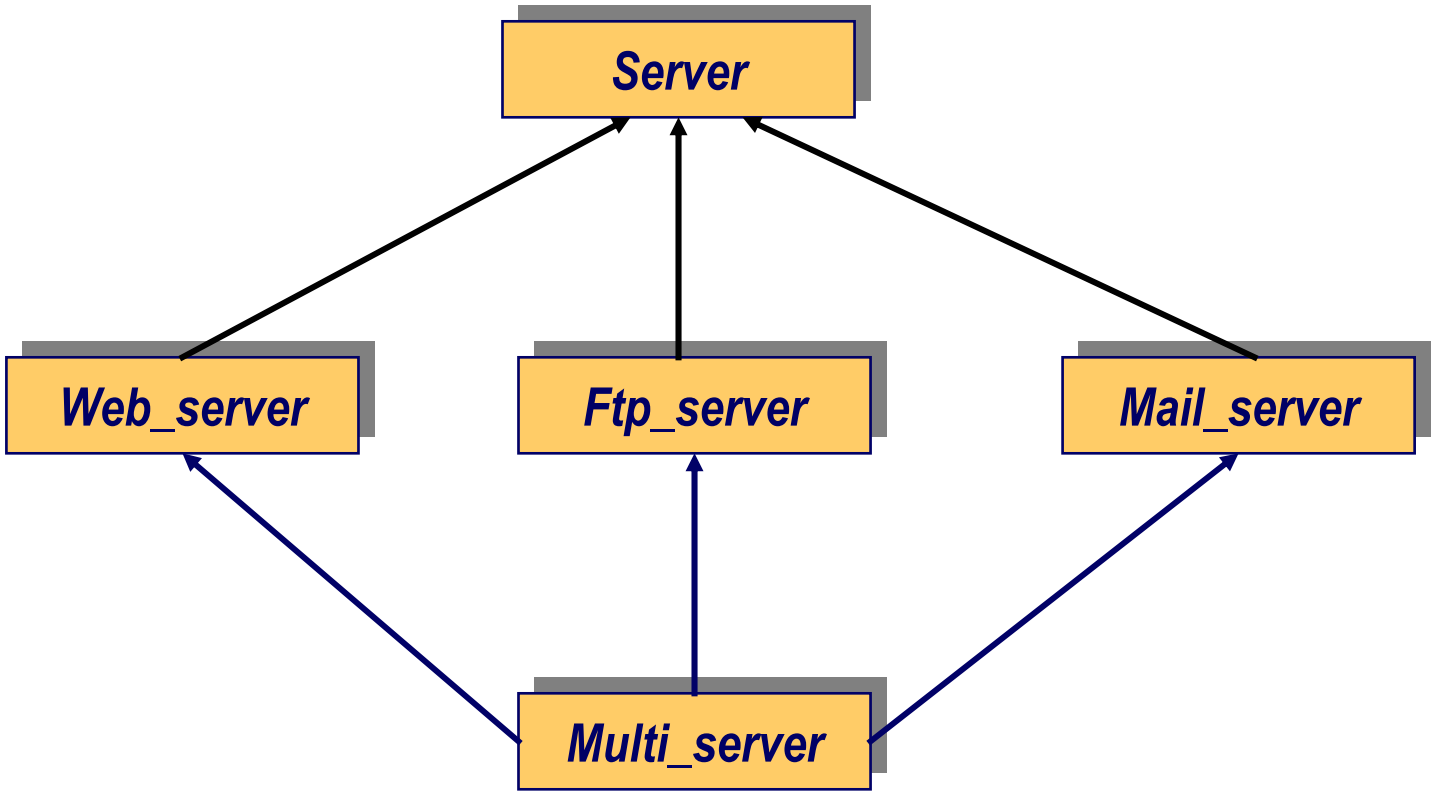
Nom_rôle	Pertinence pour *Org_fwe*	Pertinence pour *Org_fwi*
Public_host	✓	
Private_host		✓
…		
Ext_firewall	✓	✓
…		
Mail_server	✓	✓
…		
Multi_serv	✓	✓
Adm_fw_host	✓	✓
Adm_serv_host		✓

- Les rôles définis dans l'organisation *Org_LAN* ne sont pas forcément définis dans ses sous-organisations *Org_fwe* et *Org_fwi*

nora.cuppens@enst-bretagne.fr

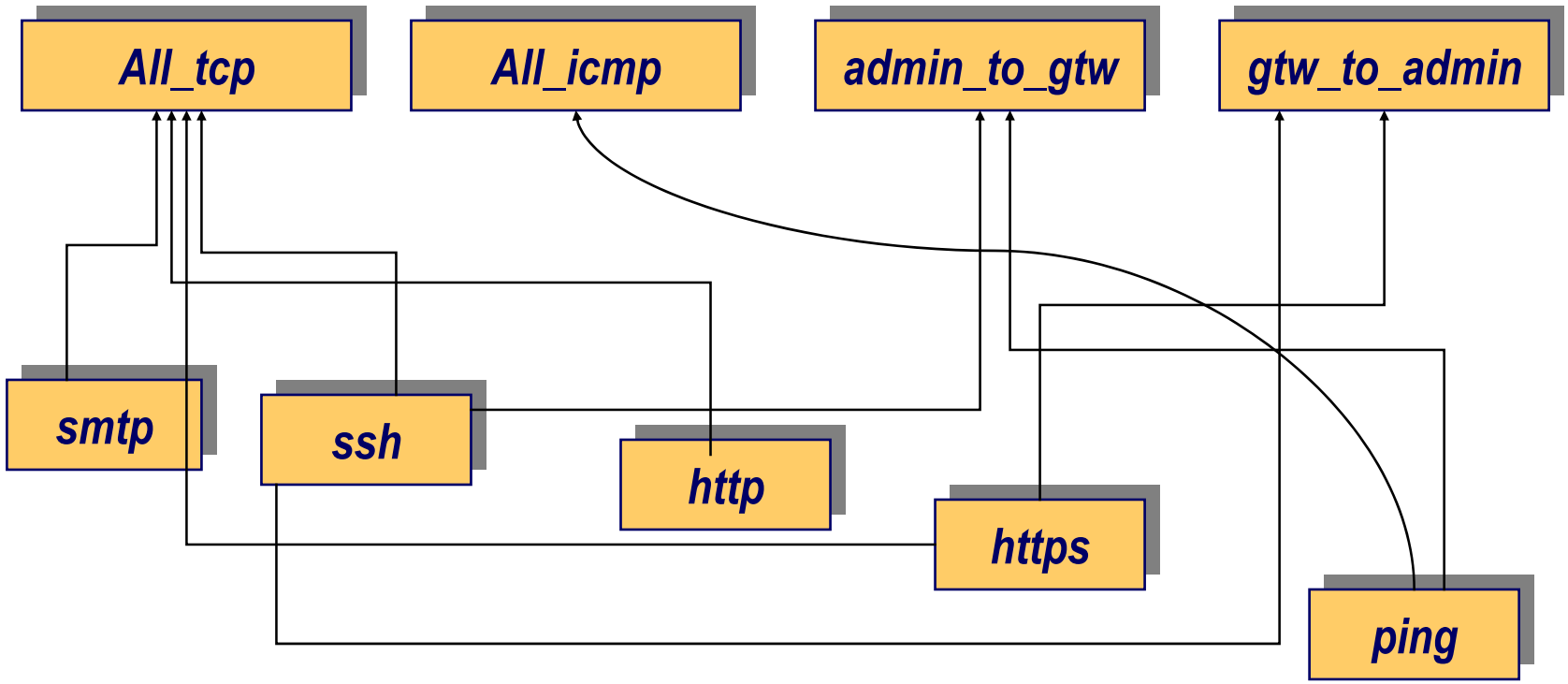
Hiérarchiser les rôles

- Notion de sous_rôle
- Spécialisation/généralisation et junior/sénior



Définir et hiérarchiser les activités

- Services offerts par le réseau local de l'*Org* anisation



nora.cuppens@enst-bretagne.fr

Définir et hiérarchiser les vues

- Ensemble des objets auxquels s'appliquent les activités
  - Vue *Target*
- Au niveau réseau, un objet *t* de la vue *Target* a deux attributs :
  - *content(t,mes)*
    - → *mes* : données transmises lors de l'utilisation du service
  - *dest(t,r)*
    - → destinataire du service identifié par son rôle (peer-role)
- Notion de sous-vue conformément au rôle du destinataire
- Dérivation des vues et sous-vues à partir des rôles et sous-rôles (*to_target(role)*)
- Dérivation de la pertinence vues/organisations à partir de la pertinence rôles/organisations

Quelques *Org_LAN_permissions*

- Permission : org × rôle × activité × vue × contexte

Permission(Org_LAN, admin_fw_host,admin_to_gtw,to-target(firewall), default)

☞ Dans l'organisation *Org_LAN*, un hôte jouant le rôle d'administrateur des firewalls a la permission d'utiliser les services d'administration des firewalls en toutes circonstances

Permission(Org_LAN, admin_server,all_tcp,to-target(multi_server), default)

Permission(Org_LAN, private_host,https,to-target(web_server), default)

Permission(Org_LAN, public_host,smtp,to-target(mail_server), default)

Dérivation des permissions

Permission(org, role, act, view, context)

$\wedge$ *sub_organization(sub_org,org)*

$\wedge$ *Relevant_role(sub_org,role)*

$\wedge$ *Relevant_act(sub_org,act)*

$\wedge$ *Relevant_view(sub_org,view)*

$\rightarrow$ *Permission(sub_org, role, act, view, context)*

nora.cuppens@enst-bretagne.fr

Quelques *Org_fwe_permissions*

☞ Dérivation à partir des hiérarchies et de l'héritage

Permission(Org_LAN, admin_fw_host,admin_to_gtw,to-target(firewall), default)

⇒ *Permission(Org_fwe, admin_fw_host,admin_to_gtw,to-target(ext_firewall), default)*

Permission(Org_LAN, public_host,smtp,to-target(mail_server), default)

⇒ *Permission(Org_fwe,public_host,smtp,to-target(mail_server), default)*

Permission(Org_LAN, private_host,all_tcp,to-target(public_host), default)

⇒ *Permission(Org_fwe,??,all_tcp,to-target(public_host), default)*

⇒ *Permission(Org_fwi, private_host,all_tcp,to-target(??), default)*

Résultats

- Spécification Or-BAC d'une politique de sécurité réseau
  - Format XML
- Décomposition de la politique
  - Politique de sécurité des composants de sécurité
- Traducteur pour générer les règles du firewall NetFilter
  - Règles traduisant des permissions
- Expression d'interdictions
  - Gestion des conflits entre permissions et interdictions
  - Niveaux de priorité associés aux permissions et interdictions
  - Résolution au niveau abstrait

Conclusion

- 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

Merci de votre attention et n'hésitez pas à nous faire part de vos interrogations maintenant …ou plus tard

nora.cuppens@enst-bretagne.fr