Sécurité des réseaux et infrastructures critiques

Anas ABOU EL KALAM

INP TOULOUSE ENSEEIHT

IRIT
CNRS - INPT - UPS - UT1 - UTM
Institut de Recherche en Informatique de Toulouse

Plan

- Parcours
- Modèles et politiques de sécurité pour les infrastructures critiques
- Modélisation des recommandations
- Mise en œuvre de politiques de sécurité et de QoS
- Évaluation des outils de sécurité
- Conclusions et perspectives

Plan

- **Parcours**

Modèles et politiques de sécurité pour les infrastructures critiques

Modélisation des recommandations

Mise en œuvre de politiques de sécurité et de QoS

Évaluation des outils de sécurité

Conclusions et perspectives

Parcours

- **Déc. 2003- Sept. 2004** : ATER

- **2004-2007** : Maître de Conférence à l'ENSI de Bourges.
  - Responsable du Département Informatique.
  - Responsable de l'option "Sécurité des Systèmes et des réseaux"

- **Depuis 2007 : Maître de Conférence à l'Institut National Polytechnique**
  - Membre élu au conseil du laboratoire
  - Membre élu au conseil du département
  - Activités de recherche et d'enseignement en sécurité des réseaux.

- Formations initiale & continue, IPST-CNAM, DGA, ...

Parcours

Évaluation des outils sécurité

- Thèse M. Gad
- Collaboration Égypte, ...

Sécurité des Réseaux Critiques

- Thèse M. Mostafa
- ADCN, ADCN+, ...

Sécurité des Infrastructures Critiques

- Thèse A. Baïna
- Projet européen CRUTIAL

Sécurité des Réseaux sans-fil, NGN

- Thèse Maachaoui
- Feel@Home

- Thèse K. Salih
- NoE NewCom++

Sécurité des Infrastructures Critiques

Sécurité des Réseaux critiques

Sécurité des Réseaux & Infrastructures critiques

Plan

Parcours

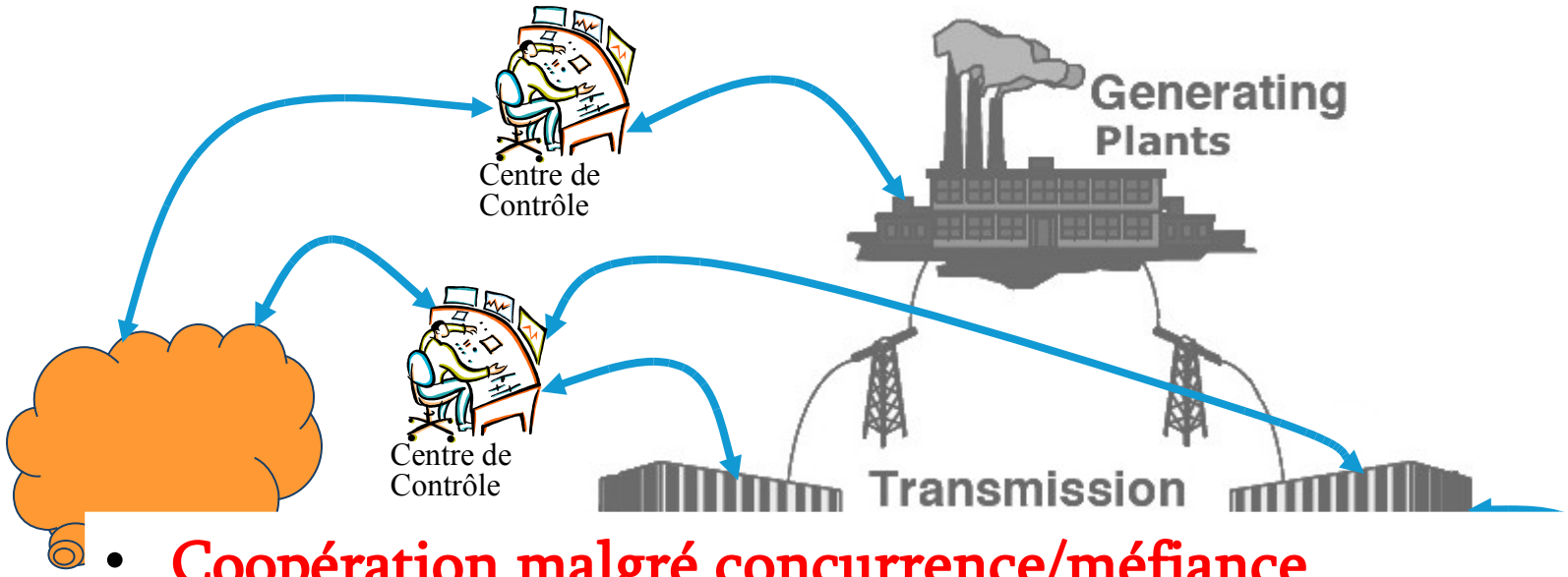
- **Modèles et politiques de sécurité pour les infrastructures critiques**

Modélisation des recommandations

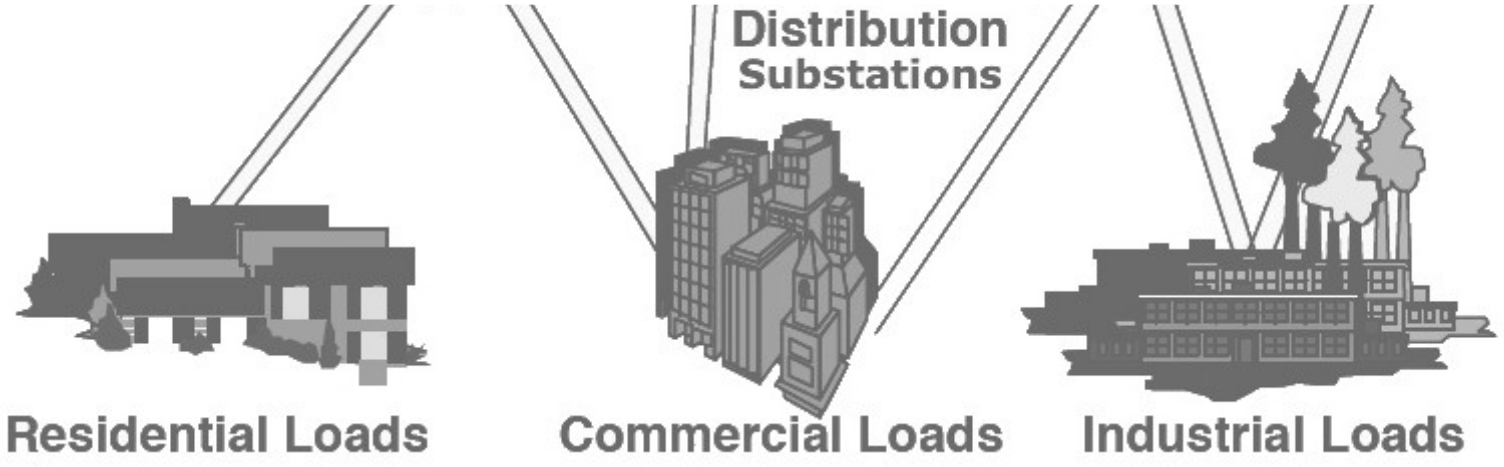
Mise en œuvre de politiques de sécurité et de QoS

Évaluation des outils de sécurité

Conclusions et perspectives



- **Coopération malgré concurrence/méfiance**
  - Interopérabilité, partage données & services
  - Indépendance et autonomie



Modèles de sécurité pour les IC

- **Politiques de sécurité**
  - Règles de sécurité qu'une organisation impose pour son fonctionnement

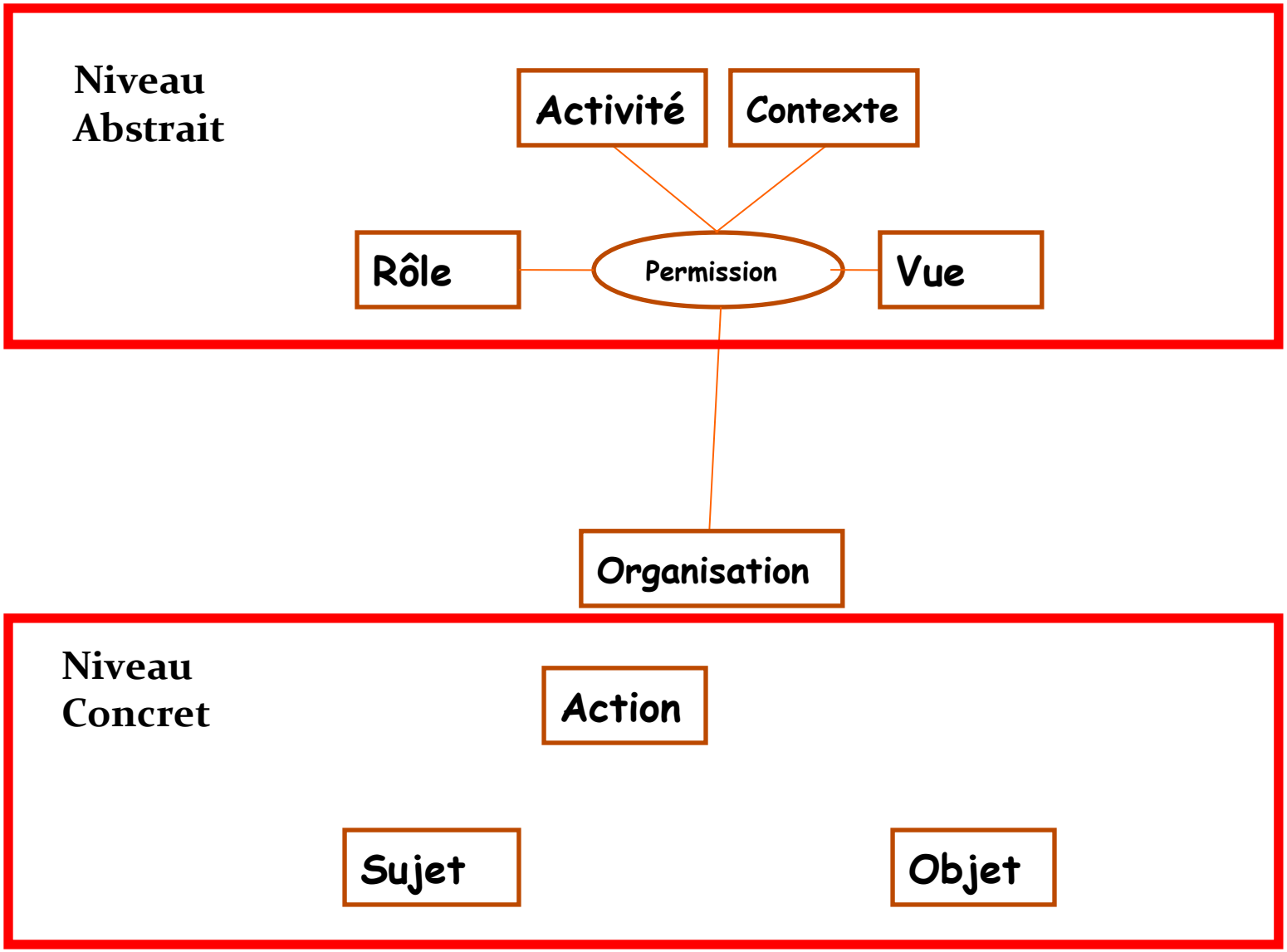
- ***Spécifiée par ...***
  - Objectifs de sécurité
  - Règles pour satisfaire ces objectifs

- ***Implémentée par ...***
  - Mécanismes d'authentification
  - Mécanismes de contrôle d'accès
  - ....

- ***Associée à ...***
  - Modèle de sécurité

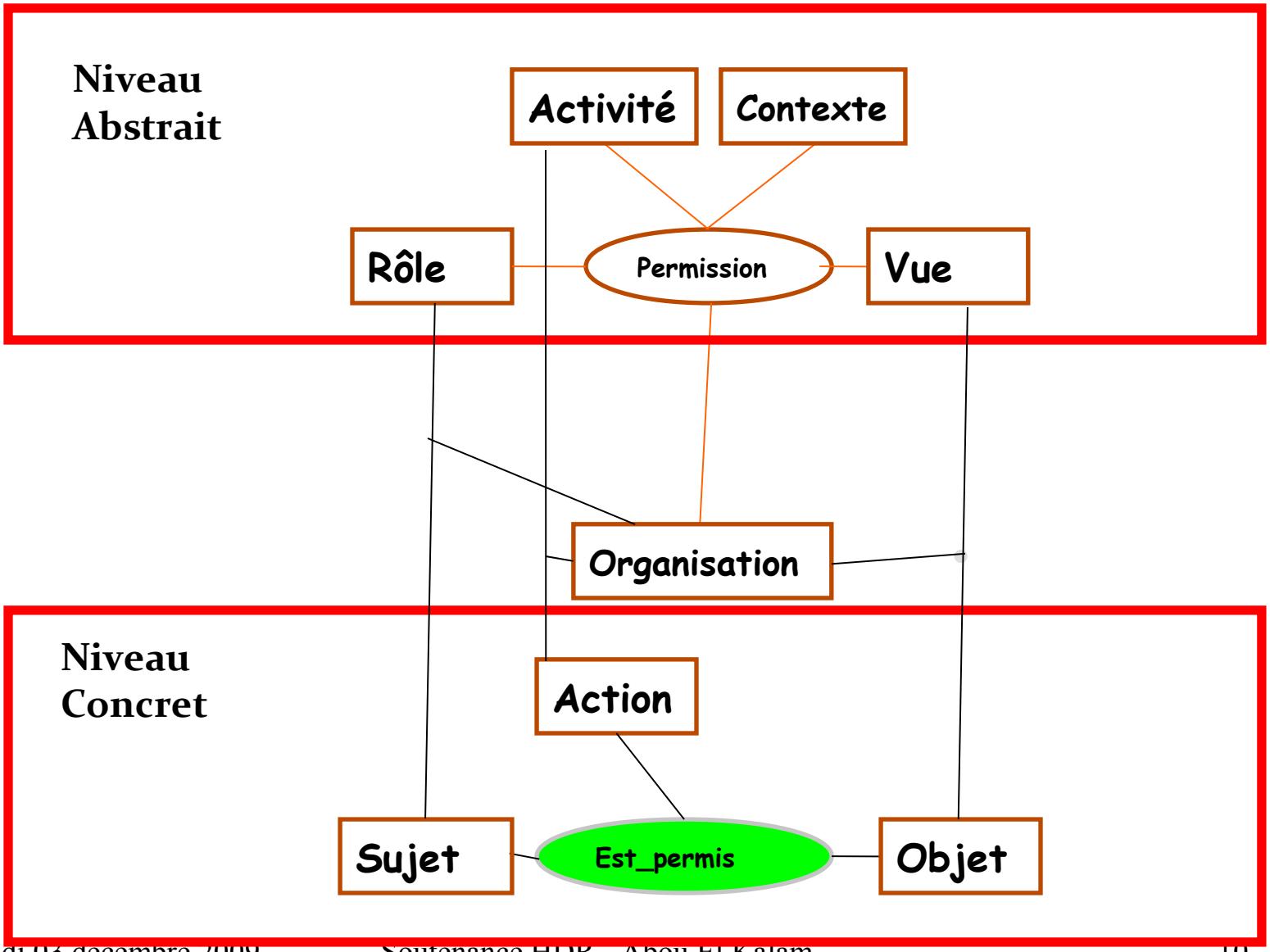
OrBAC

politique



OrBAC

politique



OrBAC

$\forall org \in Organisations, \forall s \in Sujets, \forall \alpha \in Actions, \forall o \in Objets,$
$\forall r \in Rôles, \forall a \in Activités, \forall v \in vues, \forall c \in Contextes$

Permission $(org, r, v, a, c) \wedge$
Habilite $(org, s, r) \wedge$
Considère $(org, \alpha, a) \wedge$
Utilise $(org, o, v) \wedge$
Définit (org, s, α, o, c)

$\rightarrow$ *Est_permis* (s, α, o)

OrBAC

- Avantages
  - Séparation entre politique et droits concrets
    - Mises à jours
    - Instanciation des règles
  - Règles de sécurité fines
  - Dynamicité
  - Prise en compte composants SI
  - …

- *Complexité* … ?
  - Opérations de prise de décision d'accès
  - Coûts des mises à jour
  - Risques d'erreurs

OrBAC

Est-ce adapté à notre contexte ?

Pas de mécanismes d'interaction entre organisations !!

PolyOrBAC

Thèse Amine Baina

Projet européen CRUTIAL

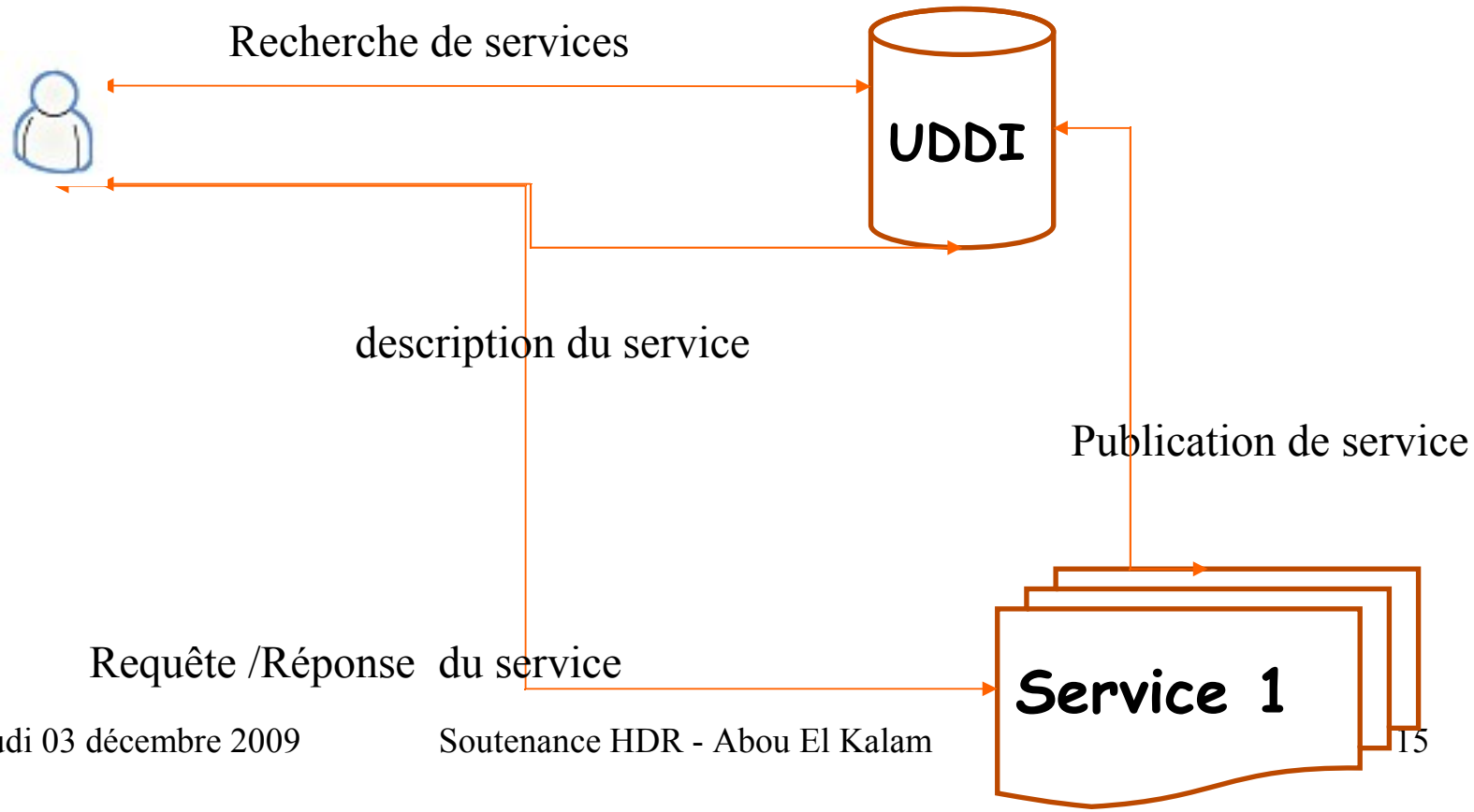
- Contrôle d'accès intra-organisation
- Collaboration inter-organisations
- Vérification temps réel des interactions

Intra-organisation

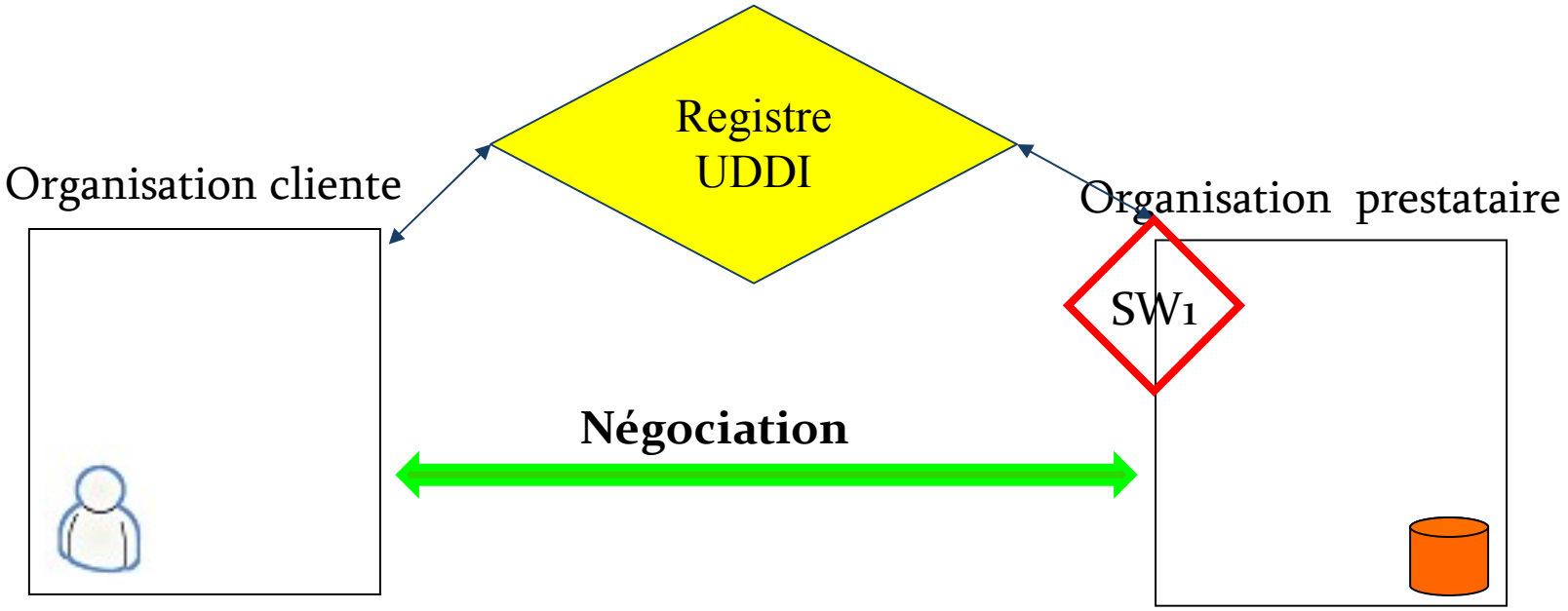
- Politiques locales spécifiées avec OrBAC
- Chaque organisation
  - Est **autonome** et **indépendante**
  - **Authentifie** ses utilisateurs
  - Est **responsable** pour les actions de ses utilisateurs
  - **Protège** ses ressources et données

PolyOrBAC : Interactions avec des SW

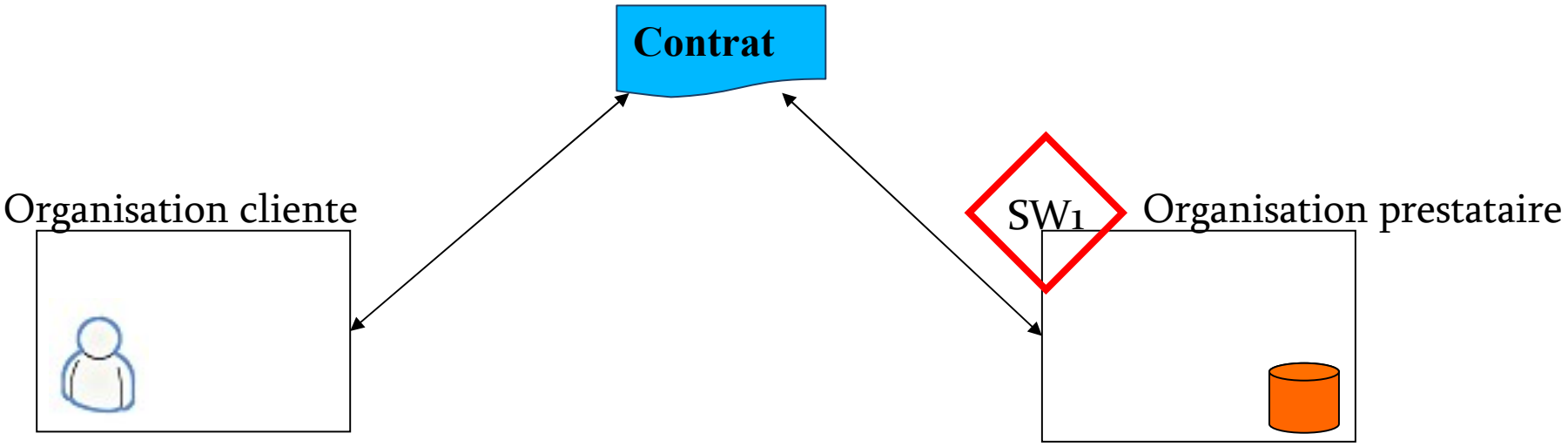
- Technologie des SW
  - Mécanismes normalisés, simples, facile d'utilisation, ...
    - Fournir ressources internes // Accès ressources externes
    - Sans divulguer l'architecture interne



PolyOrBAC : Interactions avec des SW

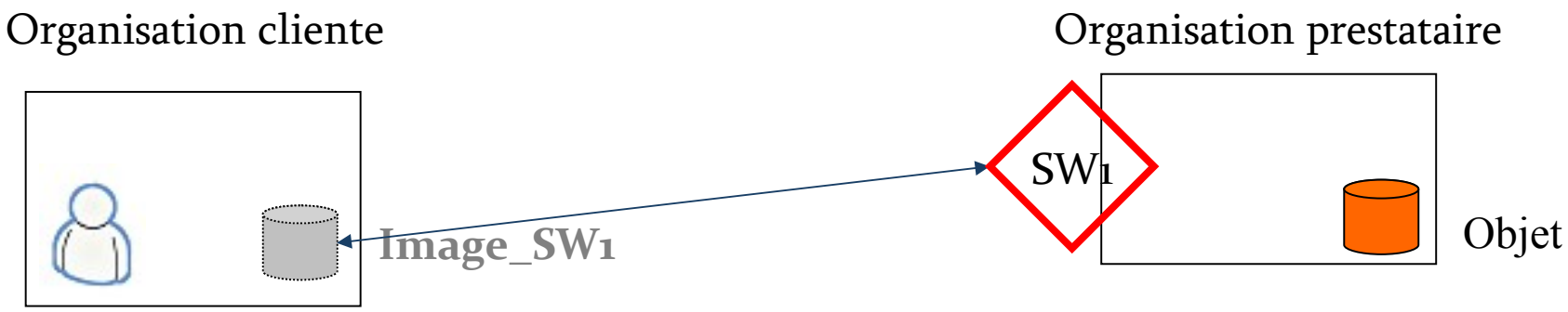


PolyOrBAC : Interactions avec des SW

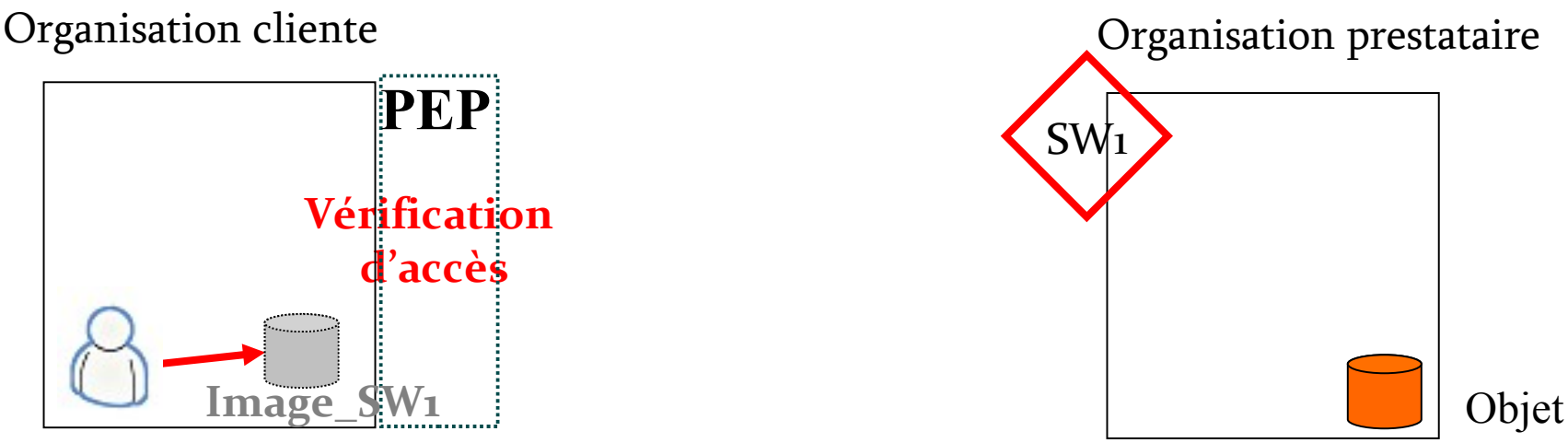


- Contrat
  - Définit protocoles, fonctions, responsabilités, paramètres, pénalités, …
  - Organisation prestataire
    - fournir le service selon le contrat
  - Organisation cliente
    - responsable des actions de ses utilisateurs

Comment gérer SW distant au niveau de l'organisation cliente ?



- Image de SW
  - Représentation (coté client) du SW distant afin de le gérer localement dans la politique de sécurité du client

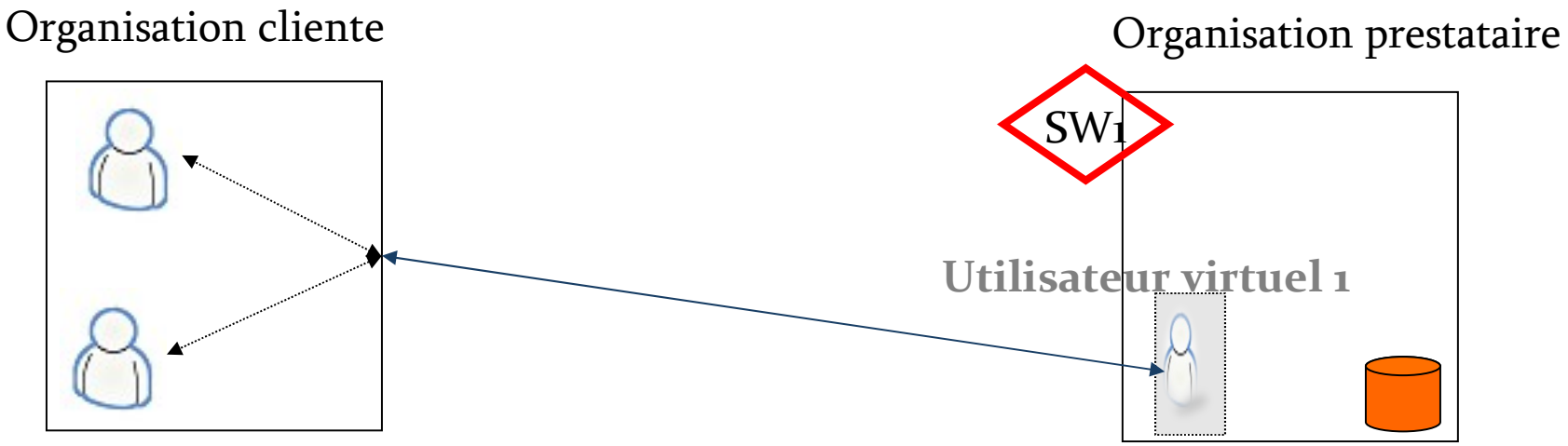


Politique OrBAC du client

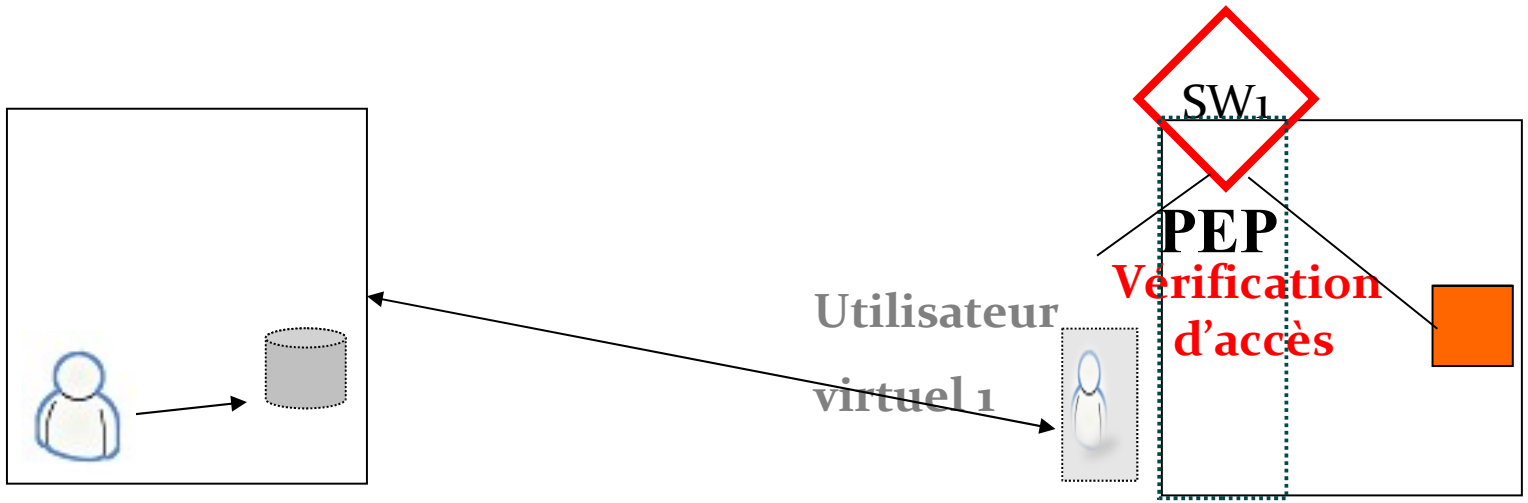
- L'appel du SW est une
- activité externe,
- représentée par un objet local virtuel (Image_SW1),
- accessible par des rôles spécifiques locaux

- Chaque organisation authentifie ses utilisateurs localement
- L'organisation client est responsable des actions de ses utilisateurs

Comment gérer utilisateurs distant au niveau de l'organisation prestataire ?



- **Utilisateur Virtuel**
  - Représentation de l'utilisateur distant coté prestataire,
  - « *virtualiser* » l'accès distant afin de le gérer comme un accès local au niveau du prestataire

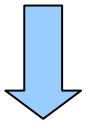


- **Politique OrBAC du fournisseur**
  - Le SW est une activité interne
  - Accessible par organisation cliente (à travers utilisateur virtuel local)
  - Avec rôle(s) ayant permission d'exécuter le SW

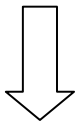
– L'organisation fournisseur est responsable de ses services

PolyOrBAC : vérification des interactions

- **Organisations mutuellement méfiantes**
  - Org. Cliente ==> *Abuse* de l'utilisation du service
  - Org. Prestataire ==> *Ne fournit pas* le service prévu avec la qualité escomptée



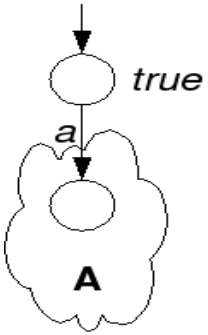
- Vérification de la légitimité des actions ?
  - Conformité action <==> contrat
  - Sinon, collecter infos ==> Désigner (en TEMPS REEL) le responsable + chemin ...



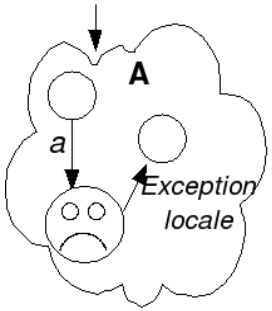
- Automates temporisés
  - Décrire les comportements de systèmes // interactions
  - Effectuer vérifications
    - Statiques, « model checking », simulations, ...

PolyOrBAC : vérification des interactions

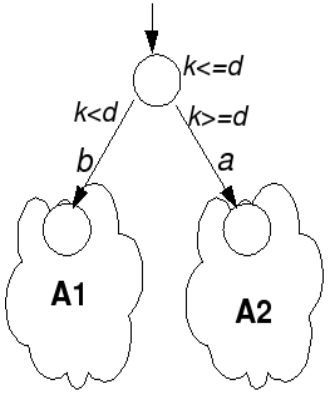
- Permissions



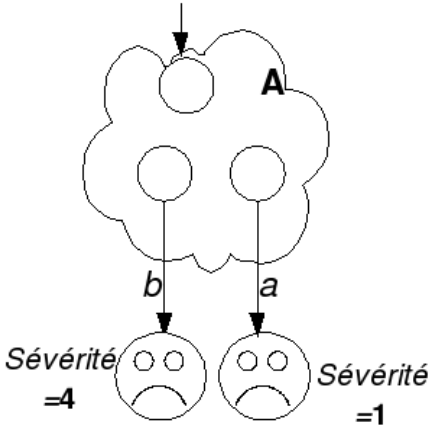
- Interdictions

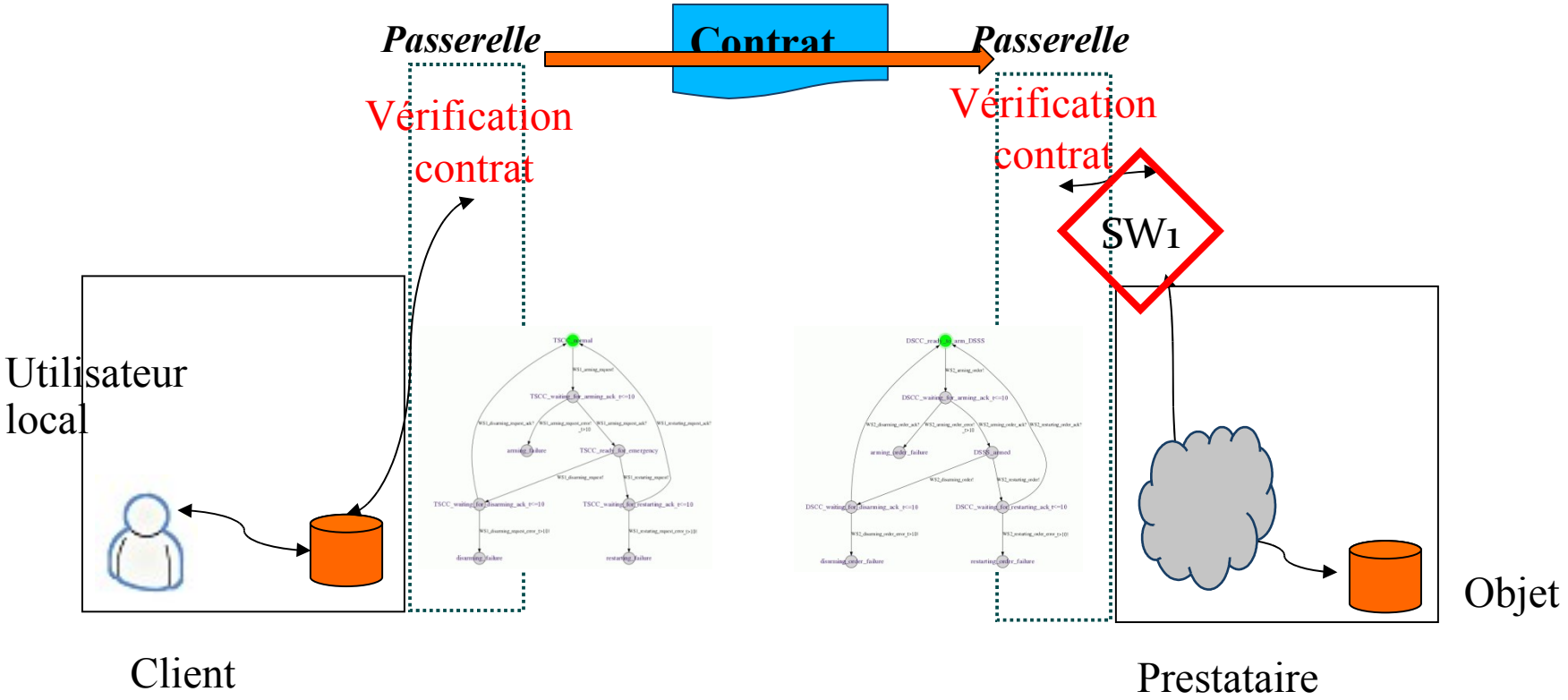


- Obligations



- Conflits





- Le contrat négocié est stocké au niveau des deux interfaces
- Chaque Interface surveille le respect du contrat.

PolyOrBAC : Récpitulatif

- Politiques de sécurité
  - modèle OrBAC
- Interactions
  - Mécanismes de services Web
  - Image de service
  - Utilisateur virtuel
- Vérification des interactions (en exécution)
  - Contrats + automates temporisés

Plan

- Parcours
- Modèles et politiques de sécurité pour les infrastructures critiques
- **Modélisation des recommandations**
- Mise en œuvre de politiques de sécurité et de QoS
- Évaluation des outils de sécurité
- Conclusions et perspectives

Recommandations

- Recommandations du "*North american Electric Reliability Council*"
- Recommandations du " *International Risk Governance Council*"
- Recommandations du "*General Assembly of United Nations*"
- Recommandations du "*Council of Europe*"
- Directives du "*European Parliament*"
- ...

Recommandations : logique déontique

Extension de la logique modale

- ∃ ==> ◊ ==> Permissions
  - $\exists x F$: *il existe une valeur possible de x tel que F est vrai ..*
- ∀ ==> ==> Obligations
- ¬ ==> Interdictions

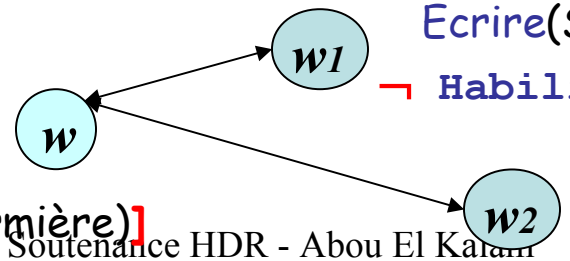
Conditions de vérité

- M,w |= **O**f ⇔ [∀w', w **R** w'] ⇒ M,w'|=f
  - f est vrai dans tous les mondes accessibles à partir de w
- M,w |= **P**f ⇔ [∃w', w **R** w'] ⇒ M,w'|=f
  - il existe au moins un monde accessible à partir de w où f est vrai
- M,w |= **I**f ⇔ [∀w', w **R** w'] ⇒ M,w'|=¬f
  - f n'est vrai dans aucun des mondes accessibles à partir de w

O[Ecrire(Sam, f1.txt)]

P[Créer(Bob, Prescription)]

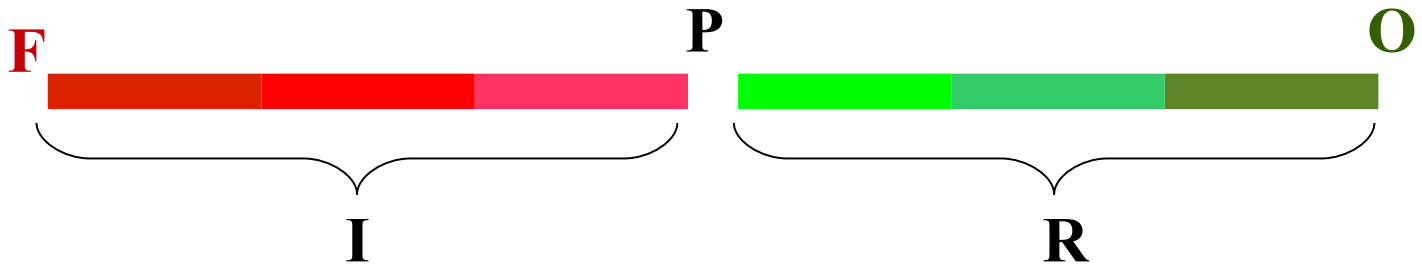
I[Habilite(org, Alice, Infirmière)]



Ecrire(Sam, f1.txt)
¬ Habilite(org, Alice, Infirmière)

Ecrire(Sam, f1.txt)
Créer(Bob, Prescription)
¬ Habilite(org, Alice, Infirmière)

RSL : syntaxe



- Syntaxe
  - $\phi ::= p \mid \neg\phi \mid (\phi \vee \psi) \mid O\phi \mid R\phi$

- Exemples
  - **R**(Read, Bob, Guide)
    - *Il est recommandé que Bob lise le guide d'utilisation*
  - **I**(Execute, Bob, OldVersion)
    - Il est déconseillé d'exécuter les versions antérieures
    - Il est recommandé de ne pas exécuter versions antérieures

$I\phi \approx R\neg\phi$

RSL : axiomatique

- *Exemple de formules qui doivent être **valides** dans notre modèle*
  - $\mathbf{O}\phi \rightarrow \mathbf{R}\phi \qquad \mathbf{R}\phi \rightarrow \mathbf{P}\phi$
  - $\mathbf{F}\phi \rightarrow \mathbf{I}\phi \qquad \mathbf{I}\phi \rightarrow \mathbf{P}\neg\phi$
  - $\neg (\mathbf{R}\phi \wedge \mathbf{R}\neg\phi)$
  - $\neg (\mathbf{R}\phi \wedge \mathbf{I}\phi)$
  - …

RSL : Sémantique

- **Semantique (définitions *intuitives*)**

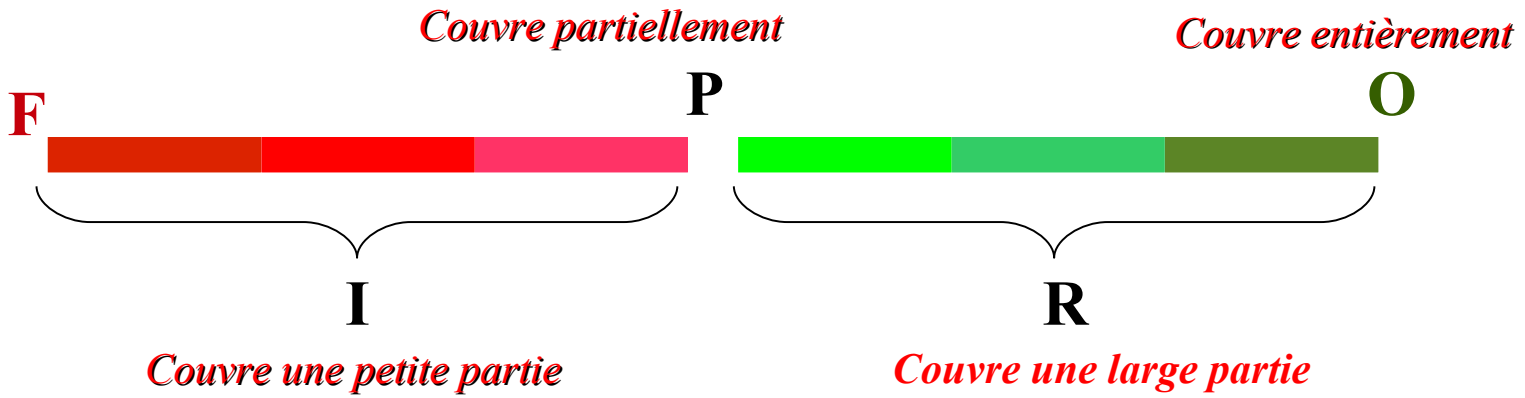
Model: $M = (W, \Re, V)$

- ϕ est Obligatoire à l'état x dans M $\Leftrightarrow$ *dans TOUS les états* $y / x\Re y$, ϕ *est vrai*
  - $\{y: \phi \in V(y)\}$ **couvre entièrement** $\Re(x)$
- ϕ est permis à l'état x dans M $\Leftrightarrow$ *dans CERTAINS états* $y / x\Re y$, ϕ est vrai
  - $\{y: \phi \in V(y)\}$ **couvre partiellement** $\Re(x)$

- ϕ is **recommandé** à l'état x dans M $\Leftrightarrow$ ***dans la PLUPART des états*** $y / x\Re y$, ϕ *vrai*
  - $\{y: \phi \in V(y)\}$ **couvre une grande partie** de $\Re(x)$

- ϕ est déconseillé ... $\Leftrightarrow$ ***dans la PLUPART des états*** $y / x\Re y$, ϕ N'EST PAS *vrai*
  - $\{y: \phi \in V(y)\}$ **couvre une petite partie** de $\Re(x)$

RSL : Sémantique

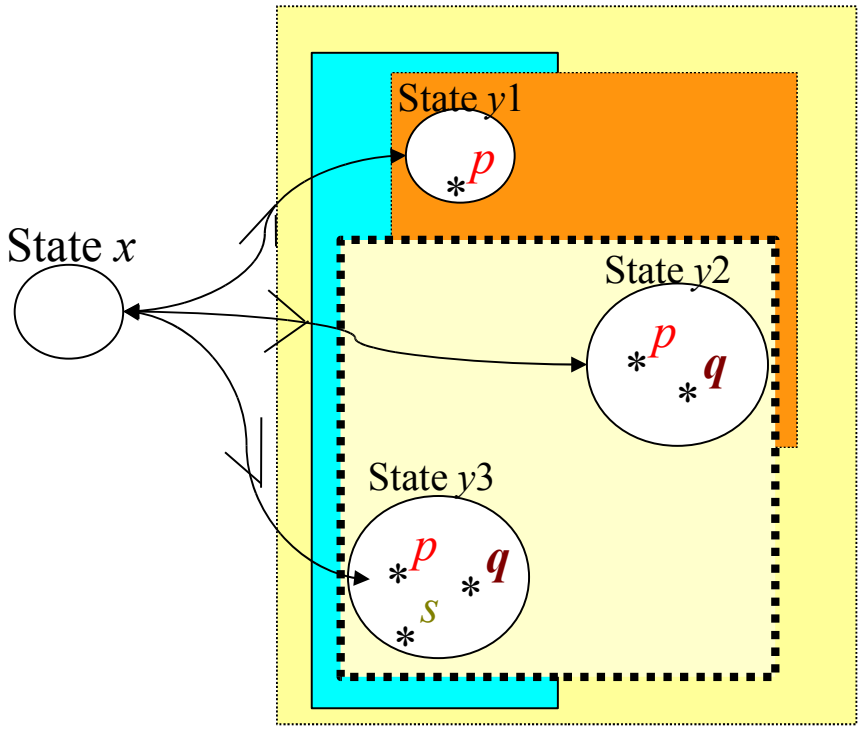


- **Semantique**

Model: $\mathcal{M} = (W, \Re, \aleph, V)$

- $\aleph$: *fonction de voisinage*
  - associe, à chaque état x, un ensemble $\mathrm{N}(x)$ de sous-ensembles de $\Re(x)$
- $\aleph(x)$ contient l'ensemble des sous-états larges de $\Re(x)$
  - ==> ensemble des recommandations dans x

RSL : Sémantique



- $\aleph(x) = \{\{y1, y2\}, \{y2, y3\}, \{y1, y3\}, \{y1, y2, y3\}\}$
- $\{y2, y3\} \in \aleph(x)$ est un sous ensemble large de $\Re(x)$,
- q est recommandé à l'état x

RSL : formules

- *Formules basiques*
  - $\mathbf{O}(\phi \rightarrow \psi) \rightarrow (\mathbf{O}\phi \rightarrow \mathbf{O}\psi)$ Axiom (K)
  - $\mathbf{O}(\phi \leftrightarrow \psi) \rightarrow (\mathbf{R}\phi \leftrightarrow \mathbf{R}\psi)$
  - $\mathbf{O}\phi \rightarrow \mathbf{R}\phi \rightarrow \mathbf{P}\phi$
  - $\mathbf{F}\phi \rightarrow \mathbf{I}\phi \rightarrow \mathbf{E}\phi$

$\approx$ $\mathbf{O}\phi = \mathbf{F}\neg\phi$, $\mathbf{P}\phi = \mathbf{E}\neg\phi$

- *Exemples de formules derivables / valides*
  - $\mathbf{O}\phi \wedge \mathbf{O}\psi \rightarrow \mathbf{O}(\phi \wedge \psi)$
  - $\mathbf{O}\phi \wedge \mathbf{R}\psi \rightarrow \mathbf{R}(\phi \wedge \psi)$
  - $\mathbf{O}\phi \wedge \mathbf{P}\psi \rightarrow \mathbf{P}(\phi \wedge \psi)$

Plan

- Parcours
- Modèles et politiques de sécurité pour les infrastructures critiques
- Modélisation des recommandations
- **Mise en œuvre de politiques de sécurité et de QoS**
- Évaluation des outils de sécurité
- Conclusions et perspectives

Parcours

Évaluation des outils sécurité

- Thèse M. Gad
- Collaboration Égypte, ...

Sécurité des Réseaux sans-fil, NGN

- Warodom, Maachaoui
- Feel@Home

- Thèse K. Salih
- NoE NewCom++

Sécurité des Infrastructures Critiques

- Thèse A. Baïna
- Projet européen CRUTIAL

Sécurité des Réseaux Critiques

- Thèse M. Mostafa
- ADCN, ADCN+, ...

Sécurité des Infrastructures Critiques

Sécurité des Réseaux critiques

Sécurité des Réseaux & Infrastructures critiques

1. Introduction

Problème 1

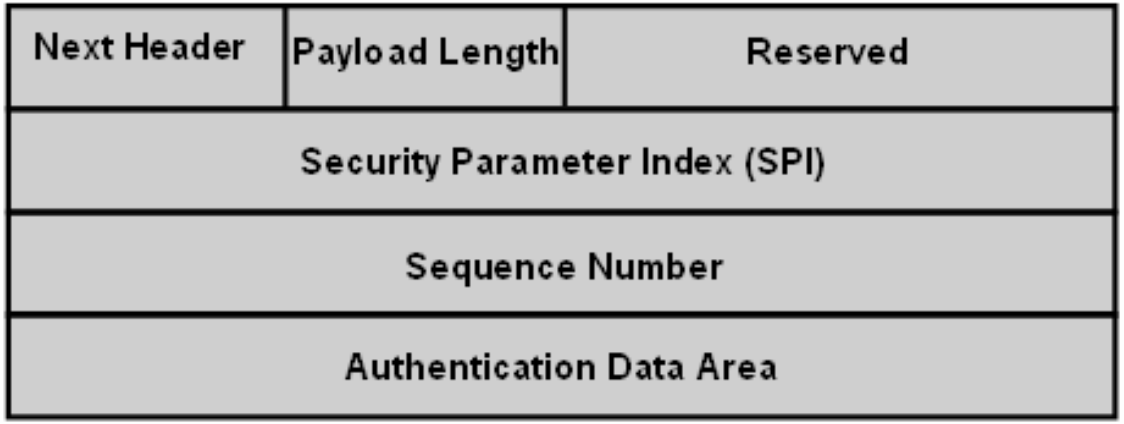
Pas de garantie de sécurité

Problème 2

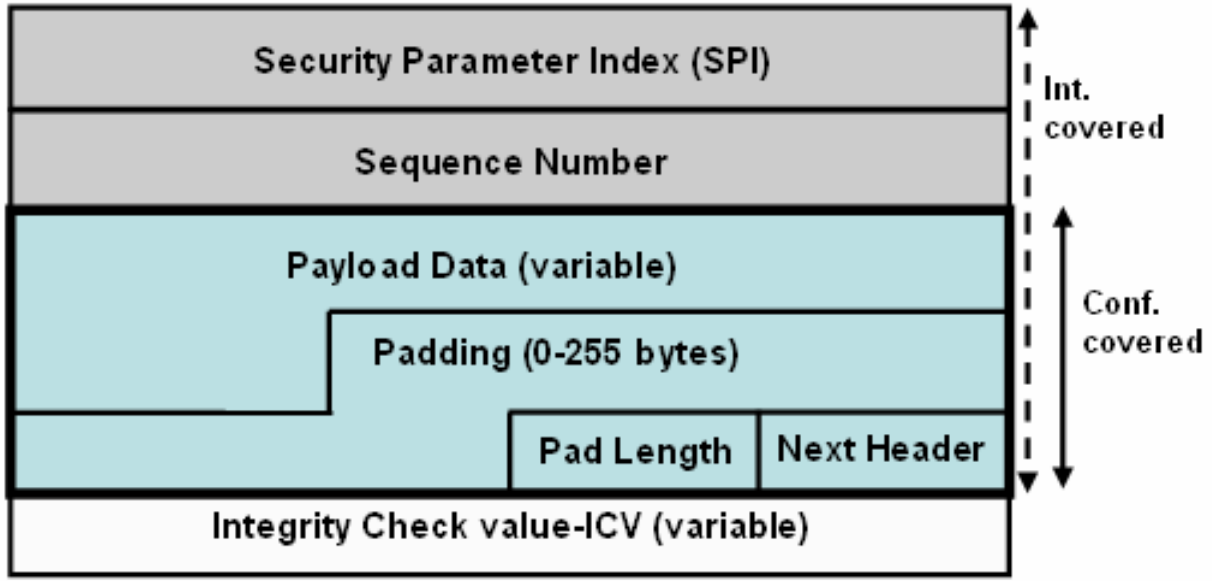
- IP traite tout le monde de manière indifférenciée
  - Toutes les données traversent un réseau IP sont routées de manière équivalente en "*best effort*"

IPSec (RFC 2401)

- AH (Authentification Header)



- ESP (Encapsulating Security Payload)

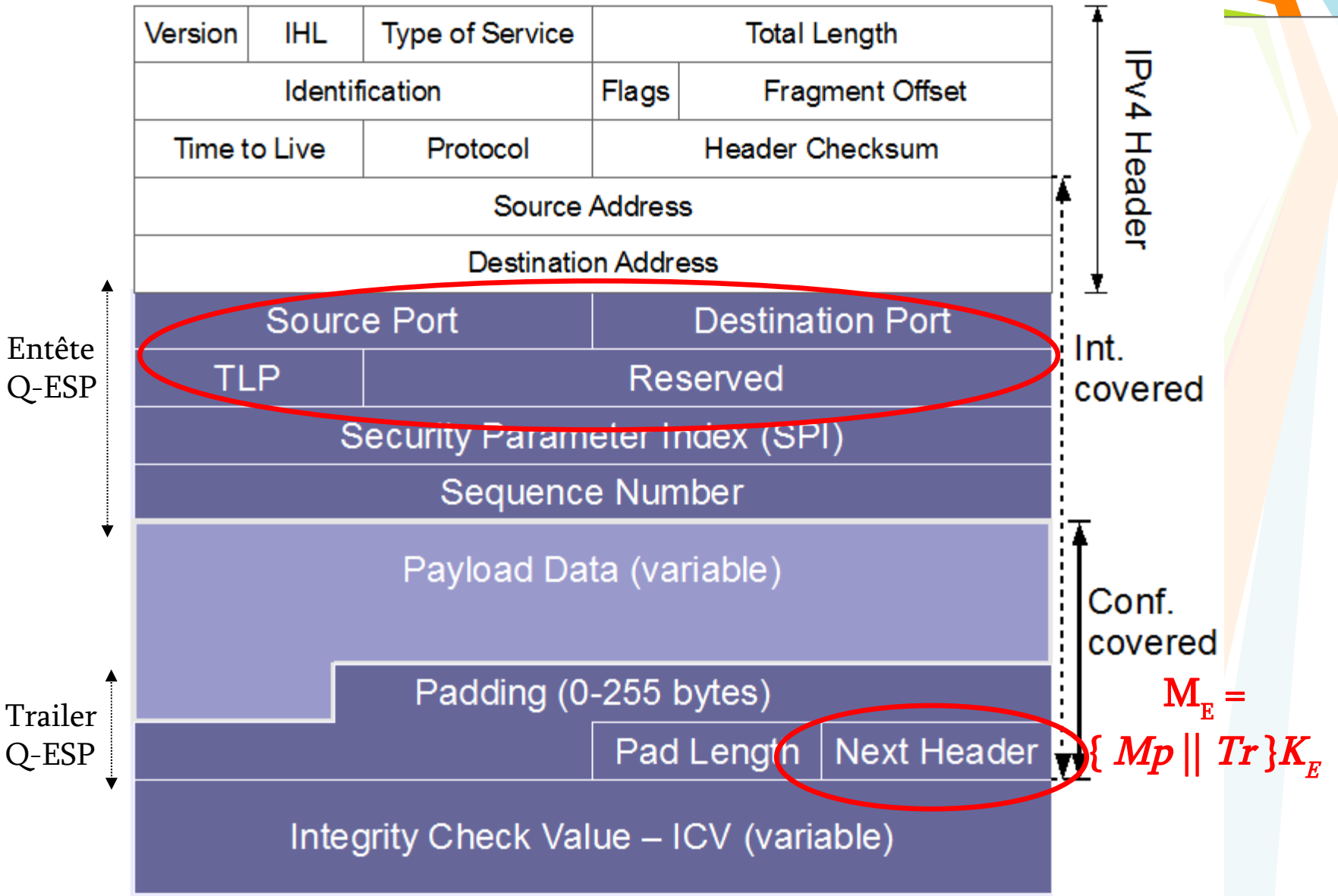


QoS Vs IPSec

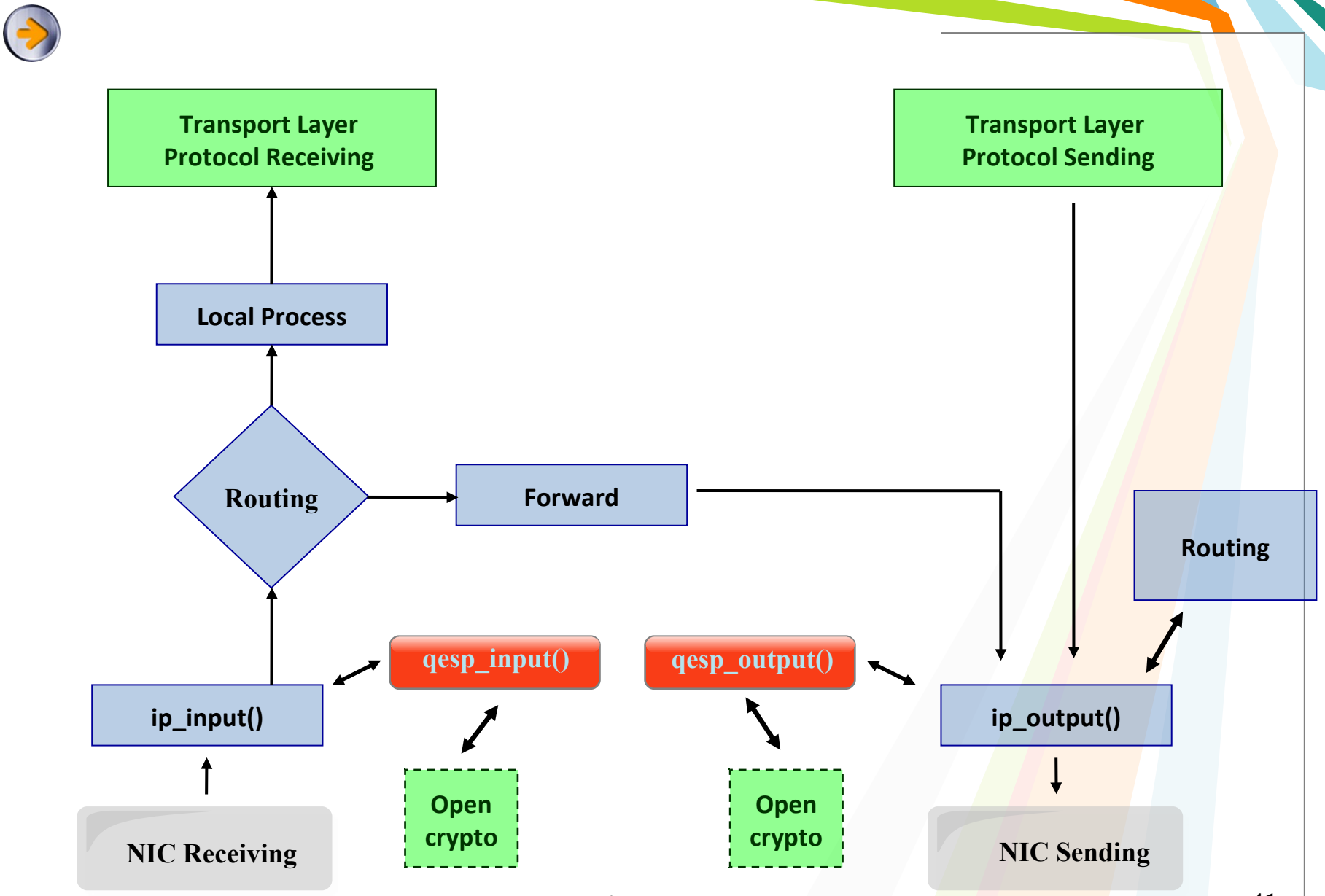
IPSec ESP ne permet pas la QoS 

- ✓ Garantir QoS ==> identifier et caractériser le trafic à l'intérieur des réseaux
  - ***Classification***
    - Niveau réseau:
      - ✓ Adresse IP source
      - ✓ Adresse IP destination
    - Niveau transport (TCP/UDP):
      - ✓ Port source
      - ✓ Destination port
      - ✓ Identifiant de protocole

Mise en œuvre de politique de sécurité & QoS

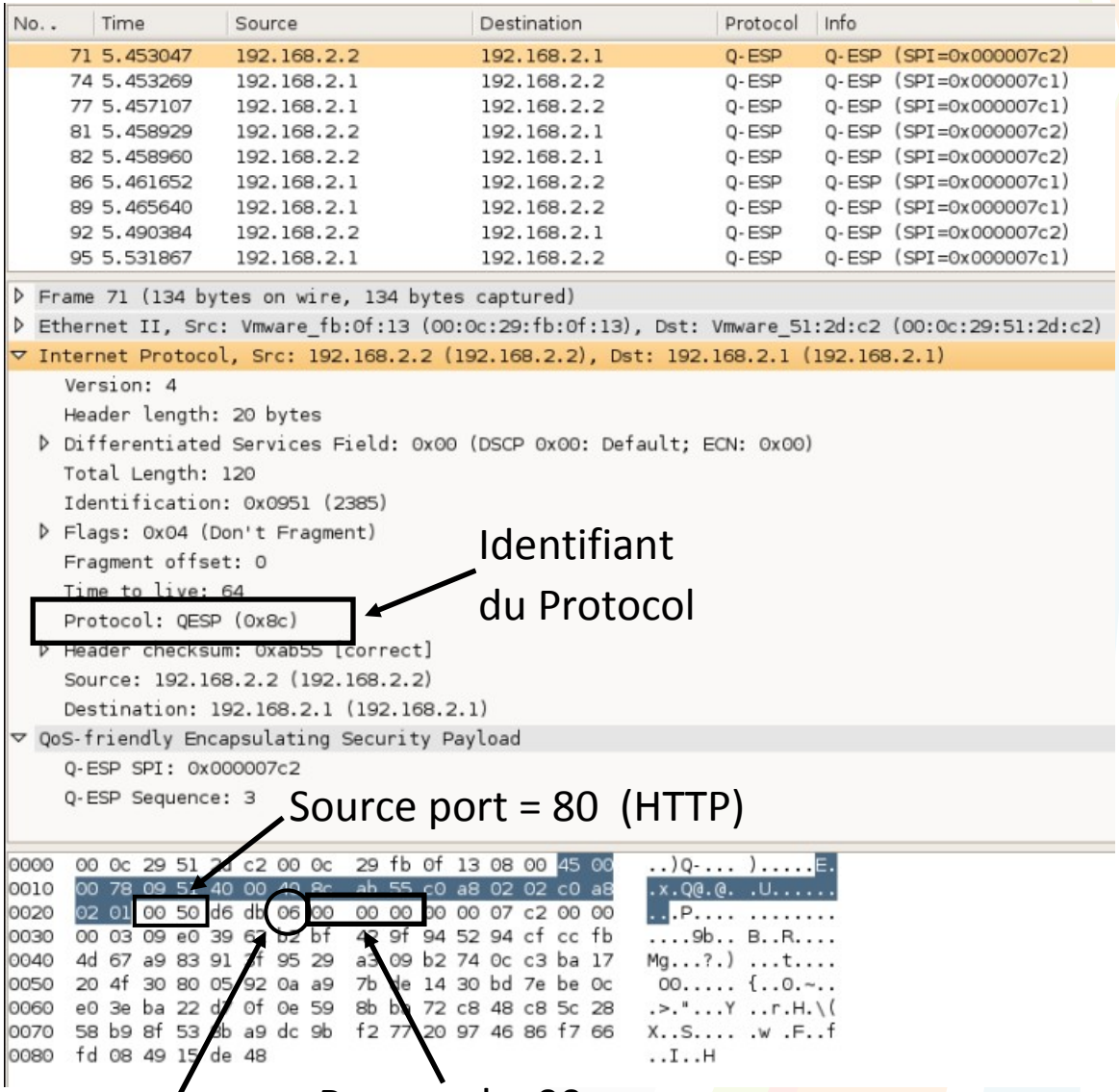


Mise en œuvre de politique de sécurité & QoS



Q-ESP: Implementation

Trafic HTTP protégé par Q-ESP en mode tunnel.



Q-ESP: Evaluation

Deux plateformes de tests

- ✓ Comparer entre IPSec ESP et Q-ESP en terme de temps de traitement.
- ✓ Prouver que ces deux protocoles sont équivalents dans un environnement *Best-Effort*

Test 1

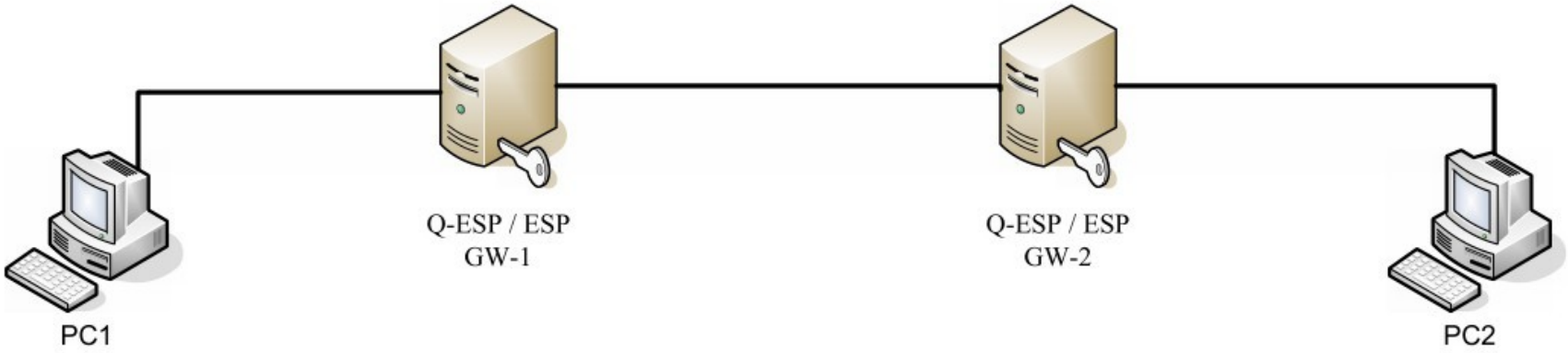
Test 2

- ✓ Mesurer les métriques QoS pour un flux temps réel protégé par ESP/Q-ESP dans une situation de congestion.
- ✓ Prouver expérimenta-lement que Q-ESP supporte la QoS.

Q-ESP: Evaluation

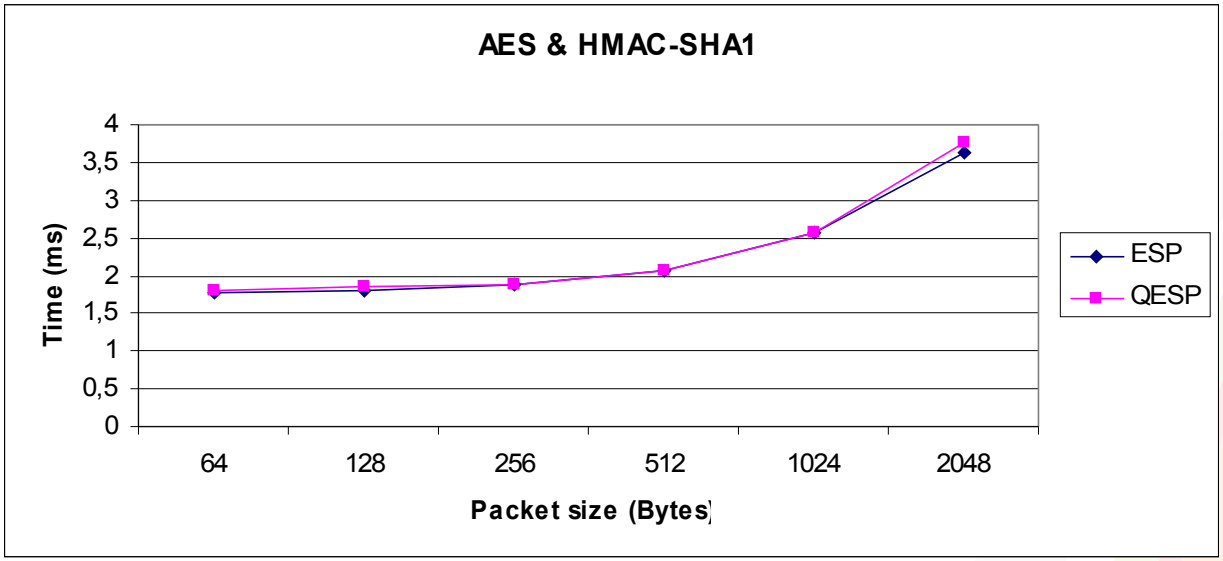
Test avec ping et l'outil MGEN, en utilisant différent algorithmes

- ✓ DES-CBC et HMAC-SHA1
- ✓ 3DES-CBC et HMAC-SHA1
- ✓ BLOWFISH-CBC et HMAC-SHA1
- ✓ AES et HMAC-SHA1



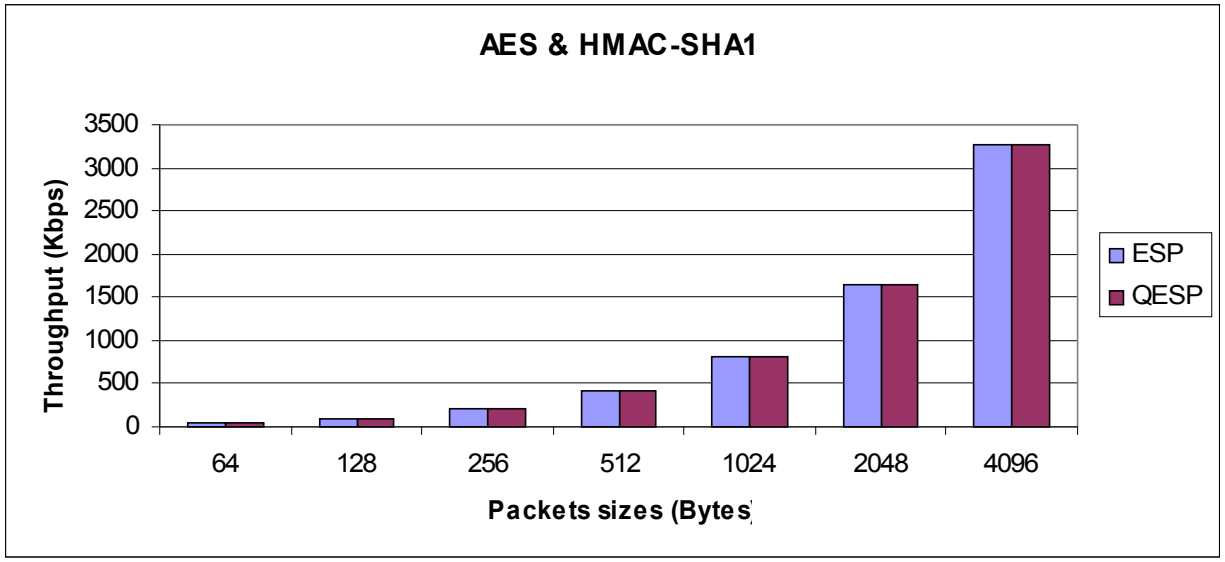
Q-ESP: Evaluation

Mesure du RTT



Q-ESP: Evaluation

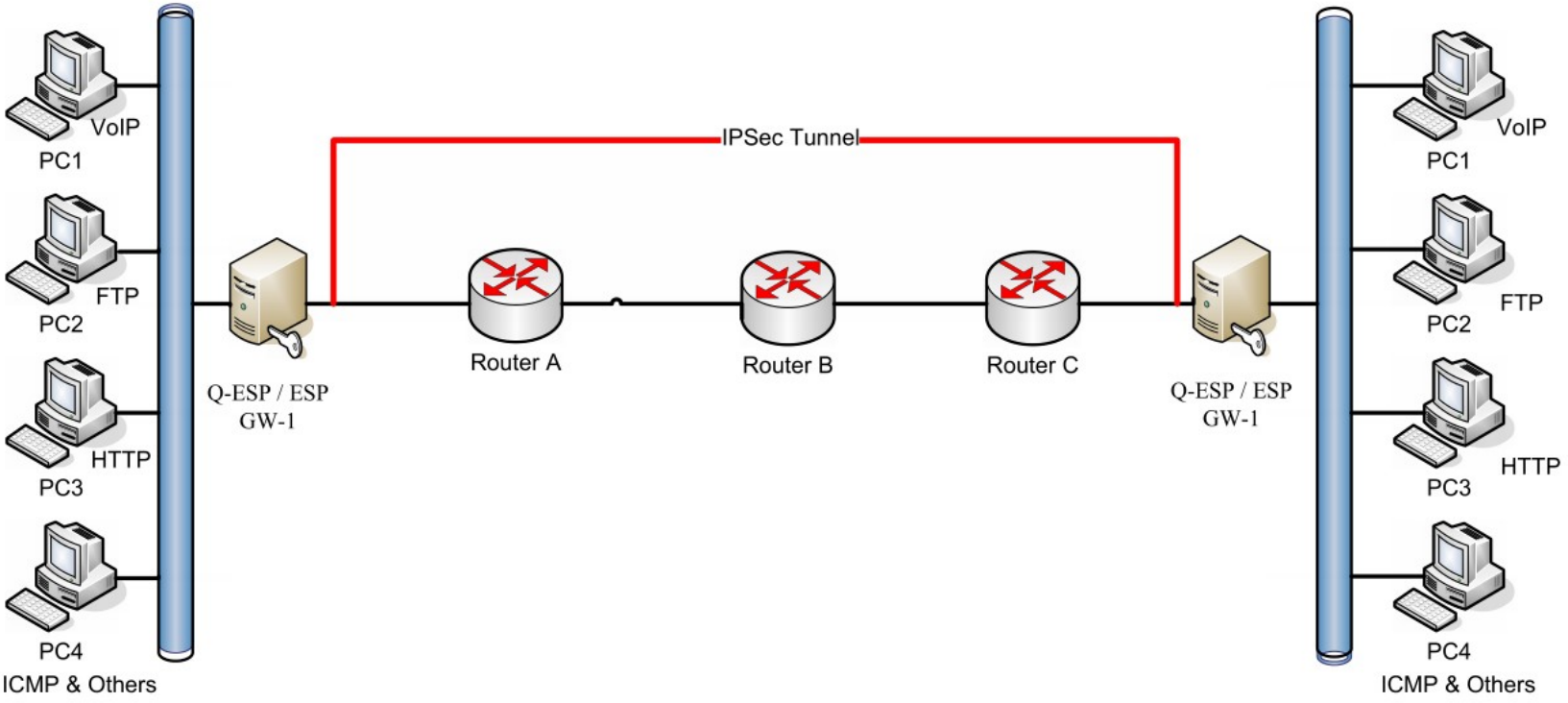
Mesure de débit (Throughput)



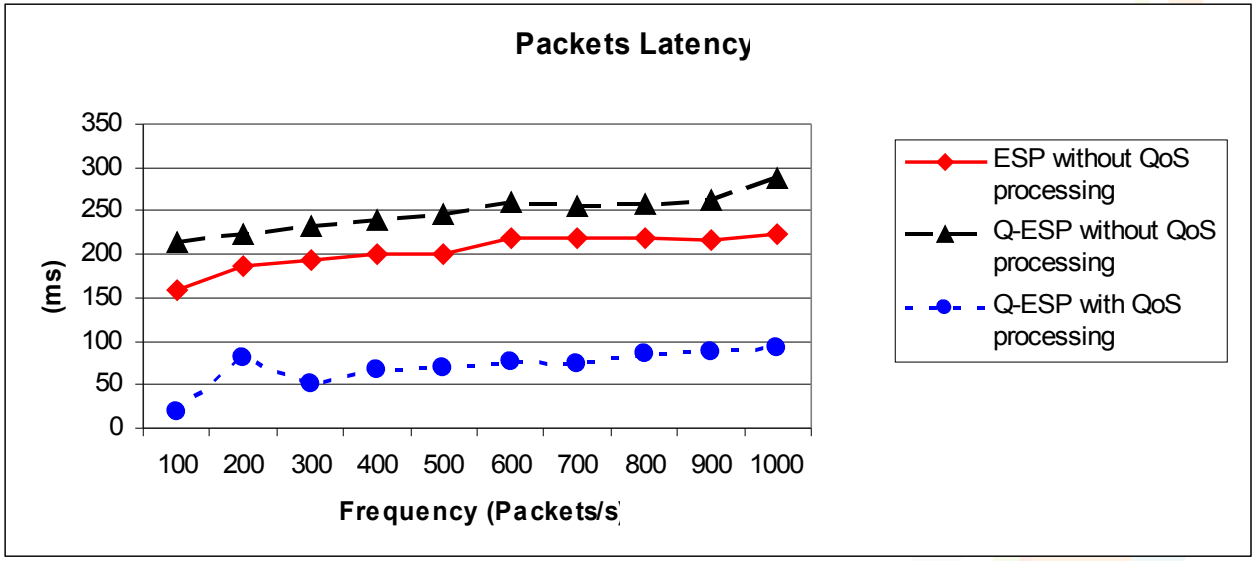
Taille des paquets	ESP	Q-ESP
64	51.243	51.191
128	102.366	102.366
256	204.715	204.834
512	409.600	409.463
1024	819.268	818.654
2048	1638.127	1637.444
4096	3275.435	3275.162

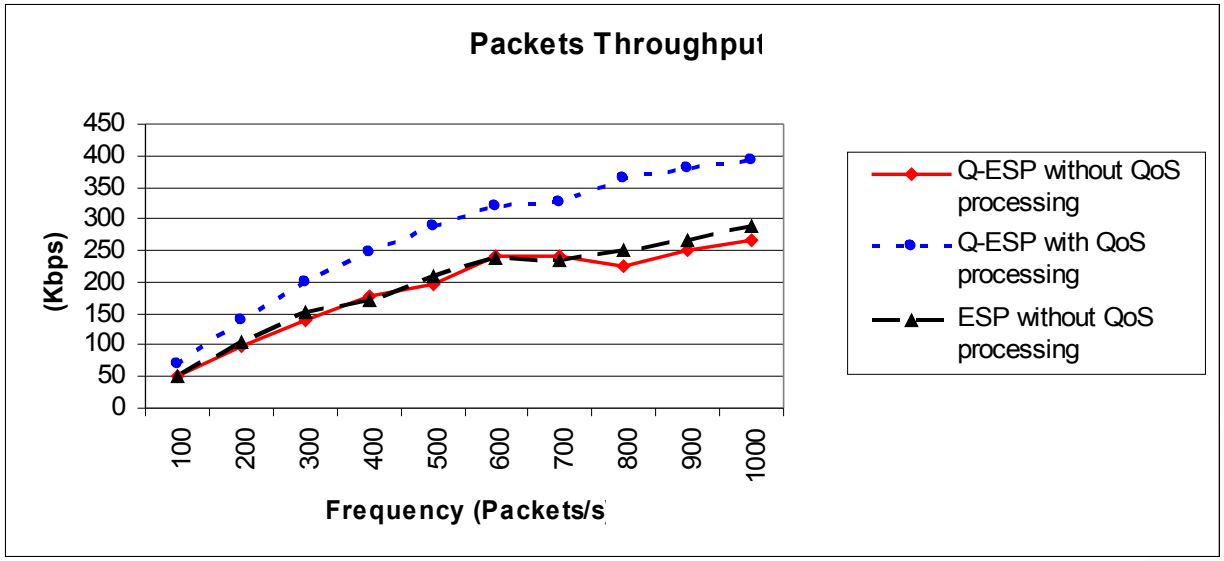
Q-ESP: Evaluation

- Mesure des métriques QoS pour ESP et
  - Q-ESP sans traitement QoS
  - Q-ESP avec traitement différencié.
- **Situation de congestion** avec les algorithmes AES et HMAC-SHA1.

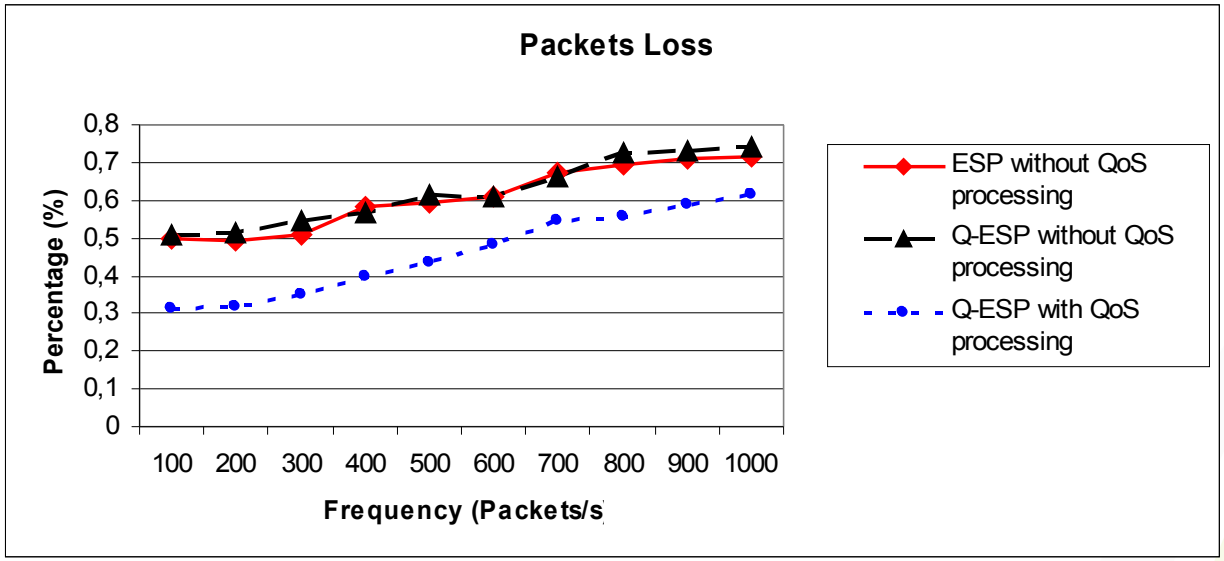


Q-ESP: Evaluation





Q-ESP: Evaluation



Plan

- Parcours
- Modèles et politiques de sécurité pour les infrastructures critiques
- Modélisation des recommandations
- Mise en œuvre de politiques de sécurité et de QoS
- **Évaluation des outils de sécurité**

Conclusions et perspectives

Parcours

Évaluation des IDS

- Thèse M. Gad
- **Collaboration Égypte, ...**

Sécurité des Réseaux sans-fil, NGN

- Warodom, Maachaoui
- **Feel@Home**

- Thèse K. Salih
- **NoE NewCom++**

Sécurité des Infrastructures Critiques

- Thèse A. Baïna
- **Projet européen CRUTIAL**

Sécurité des Réseaux Critiques

- Thèse M. Mostafa
- **ADCN, ADCN+, ...**

Sécurité des Infrastructures Critiques

Sécurité des Réseaux critiques

Sécurité des Réseaux & Infrastructures critiques

Évaluation des IDS

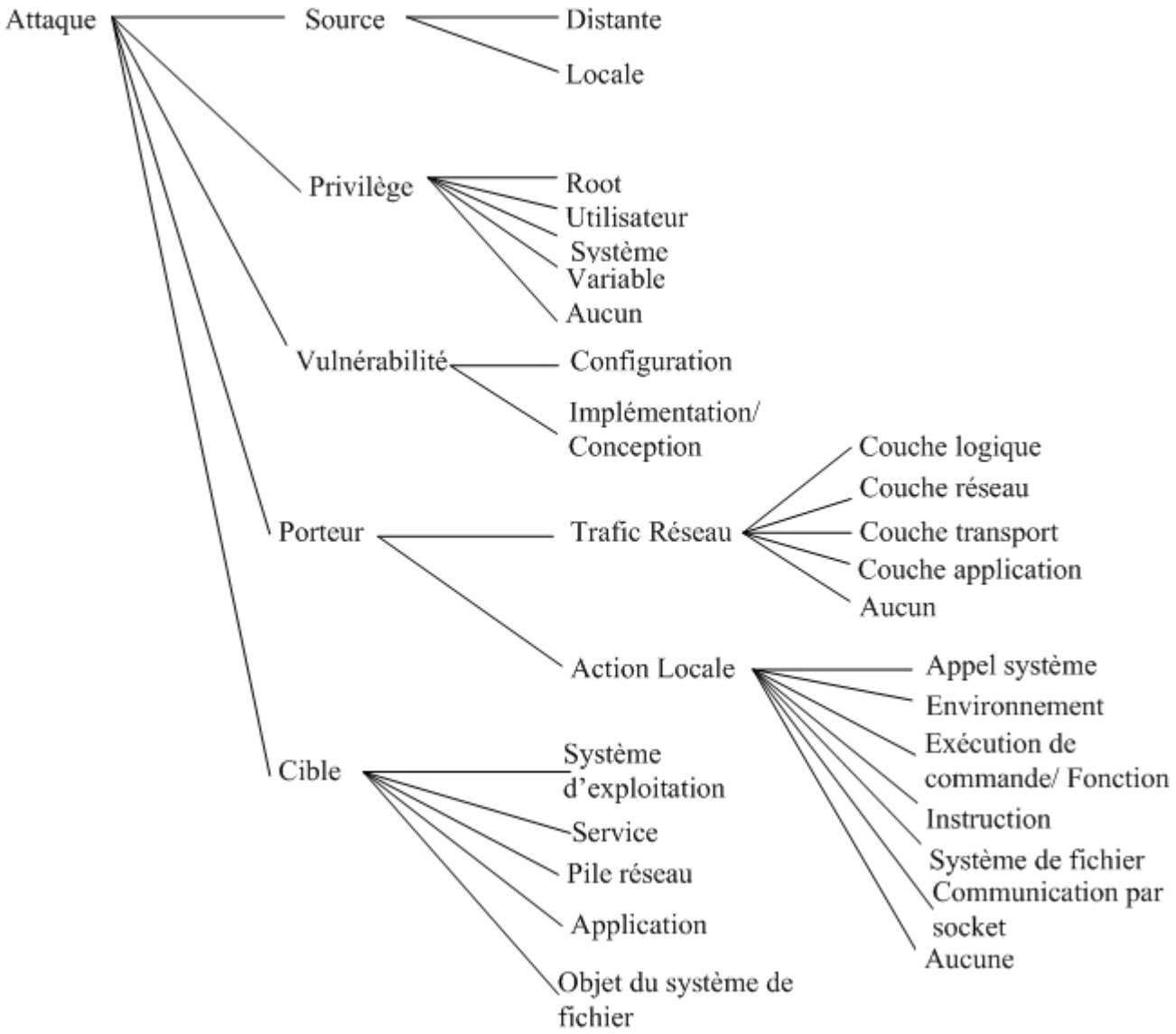
- Comment évaluer l'efficacité / robustesse outils de sécurité (IDS) ?

- Créer des *données réalistes de test* ...
  - Traffic de fond
  - Traffic malveillant

- Deux problèmes
  - Classifier de manière pertinente les attaques ?
  - Générer des scénarios représentatifs d'attaques ?

Évaluation des IDS

Classification des attaques



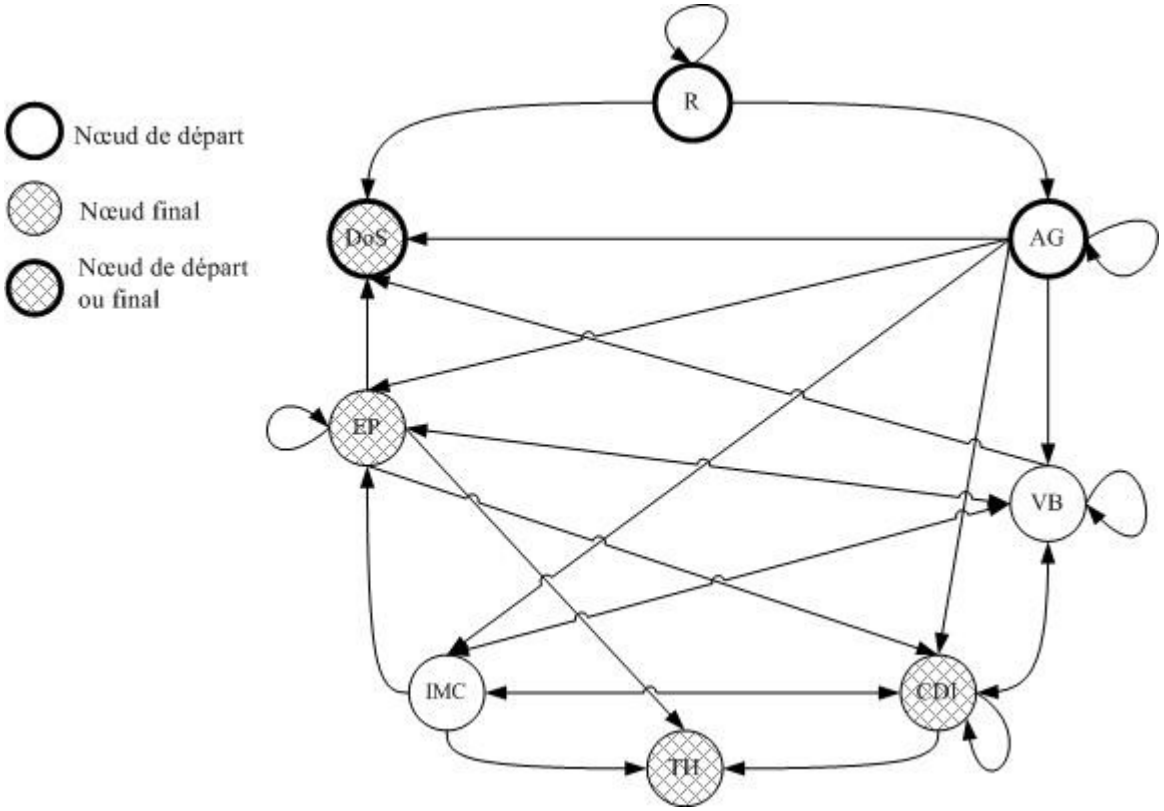
Évaluation des IDS

Processus d'attaques

- Incidents de sécurité : **manque de données**
- Données de processus d'attaques : **incompletes**

- Analyse d'attaques automatiques (viruses et vers)
  - Données disponibles
  - Complets, “self contained attack”
  - Idée sur le processus “complet”

Processus d'attaques



Exemples

- Scenario(XSS) = {R, GA, EP}
- Scenario(Mitnick) = {GA, IMC, EP}

Évaluation des IDS

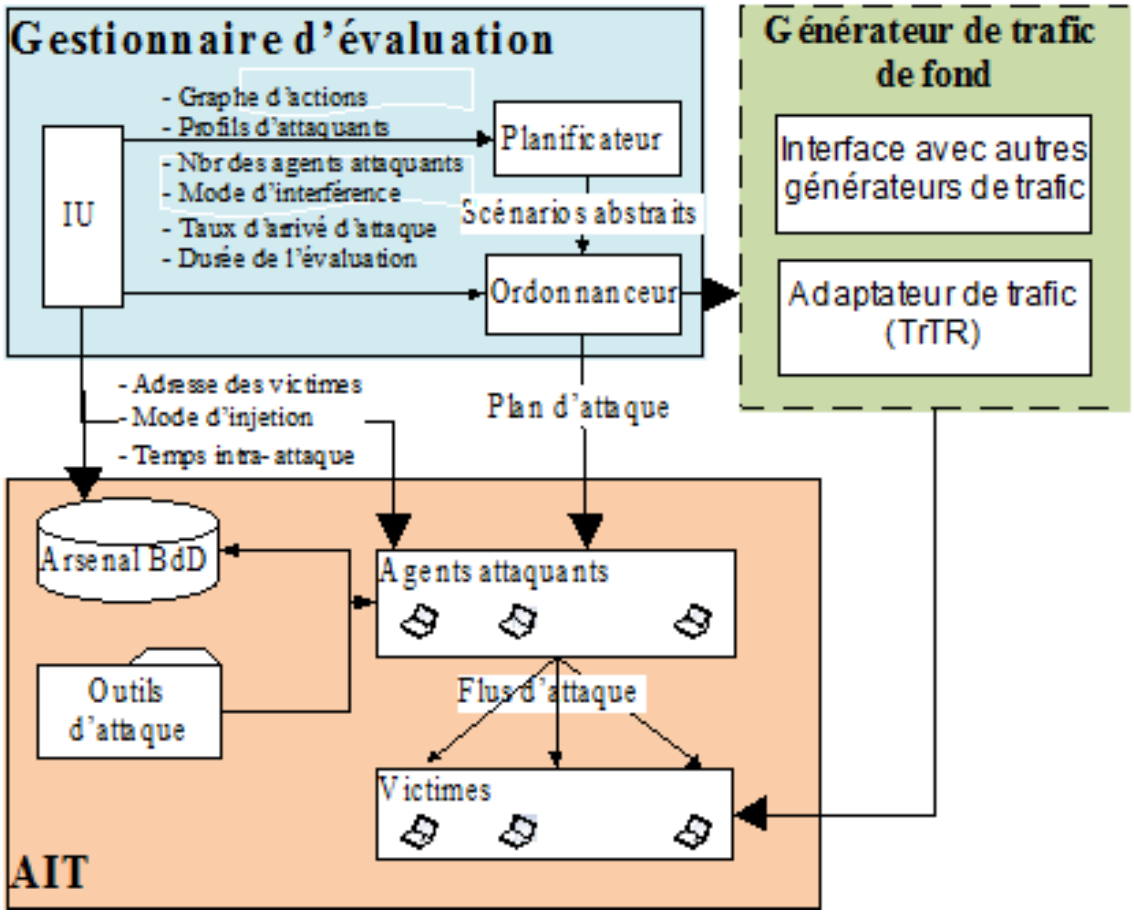
Génération trafic d'attaques

- Transformer scénarios abstraits **en séquences exécutables**
  - **Mappage** : étapes abstraites <==> commandes / outils capables de les réaliser
    - **R** ==> (nessus, nmap, ping, traceroute, etc.)
    - **VB** ==> (ls, ps, uname, etc.)
    - **AG** ==> (SSH, telnet, execute a metasploit vulnerability, etc.)
    - **CDI** ==> (cp, rm, mv, edit fichier config, change var environment)
    - **EP** ==> (malicious, crontab, lynx, nc, etc.)
    - **TH** ==> (rm log, kill syslog, kill antivrirus process etc.)
    - **DoS** ==> (shutdown –halt, crash system, stop service, etc.)
    - **IMC** ==> (scp malicious, ftp malicious, éxecuter metasploit avec payload malveillant, …)

Évaluation des IDS

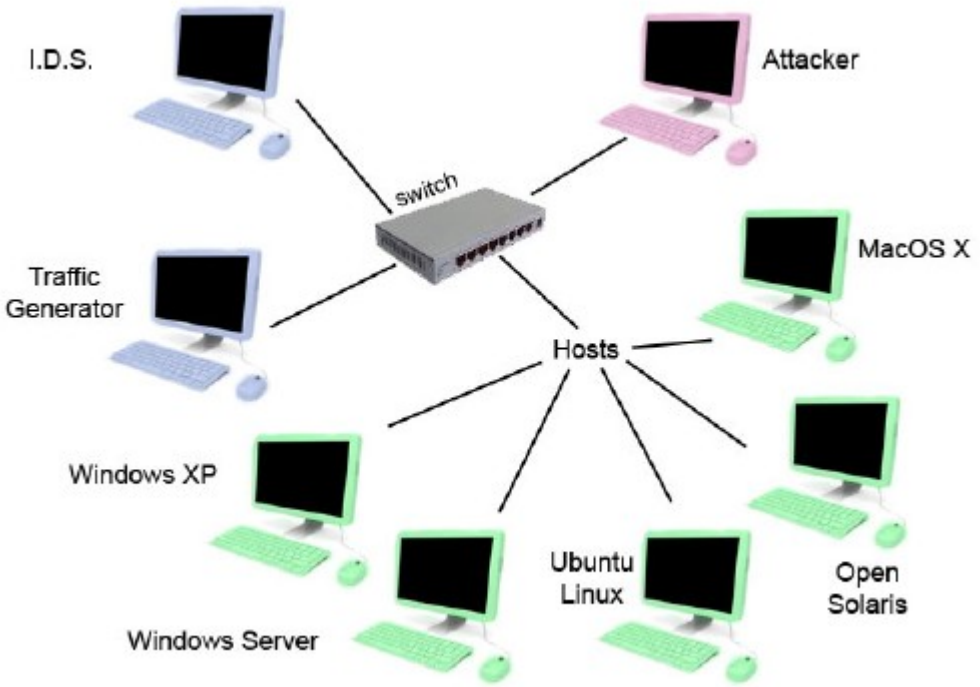
- Exemple : commande « *ping* » :
  - *Source* : distante ;
  - Privilège obtenu : aucun ;
  - *Vulnérabilité* : configuration ;
  - *Porteur* : réseau, niveau transport ;
  - *Cible* : Pile réseau ;
  - *Étape de l'attaque* : Reconnaissance.

Architecture & Implémentation



Évaluation des IDS

Plateforme de test



Benchmarking Bro & Snort

- *Unregistered rules* : règles fournies par les membres non-enregistrés sur le site de Snort,
- *Registered rules* : règles fournies par les membres enregistrés sur le site de Snort,
- *Community rules* : règles mises à jour régulièrement par la communauté de Snort,
- Community + Unregistered rules,
- Community + Registered rules,
- *Emerging rules* : règles gratuites fournies par la communauté open-source *Emerging threats*
- *Best* : ensemble de toutes les règles précédentes

Évaluation des IDS
Résultats de qlq tests de snort

- Attaques contre IIS
  - aucune des règles gratuites ne permet de les détecter toutes
  - les différences entre les capacités de détection des différents ensembles de règles restent très minimes
  - la combinaison de touts les ensembles ne permet de détecter qu'une attaque de plus par rapport aux règles fournies par les membres non-enregistrés.
- Attaques contre services Windows
  - *Registred rules* sont nettement mieux que les *Unregistred rules* + *Community rules ;*
  - *Community + registred* ont le même taux de détection que l'ensemble de toutes les règles
  - Même dans les meilleurs cas, 50 % des exploits ne sont pas détectés !
  - aucun des ensembles des règles ne permet de détecter les exploits récents !
- Attaques contre Savant
  - Détecteé mais mal identifié

Évaluation des IDS
Résultats de qlq tests de Bro

- Attaques contre IIS
  - Bro détecte 5 sur les 9 exploits injectés
    - *… meilleur que Snort
- Attaques contre les services Windows
  - Bro ne détecte aucune des attaques !

Plan

- Parcours
- Modèles et politiques de sécurité pour les infrastructures critiques
- Modélisation des recommandations
- Mise en œuvre de politiques de sécurité et de QoS
- Évaluation des outils de sécurité
- **Conclusions et perspectives**

Conclusions

- PolyOrBAC

• *gérer, de manière sécurisée, les interactions entre des organisations qui collaborent dans un environnement de suspicion mutuelle, distribué, hétérogène et dynamique*

  - OrBAC
  - SW
  - Automates temporels et model checking

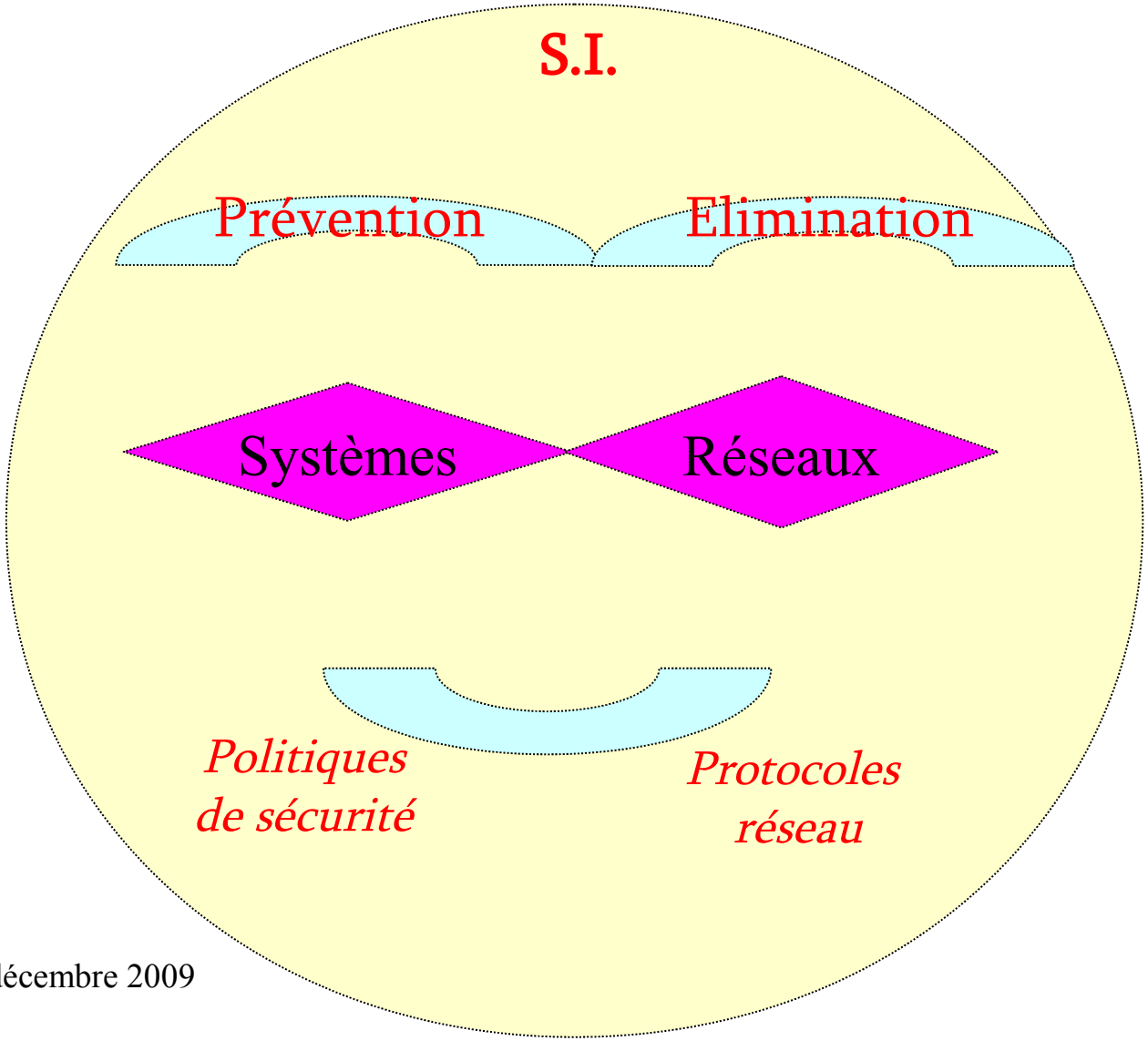
- RSL
  - Syntaxe
  - Sémantique
  - Axiomatique & règles d'inférence

- Q-ESP
  - Sécurité & QoS

- AIT
  - Evaluation des IDS
  - Classification
  - Processus d'attaques

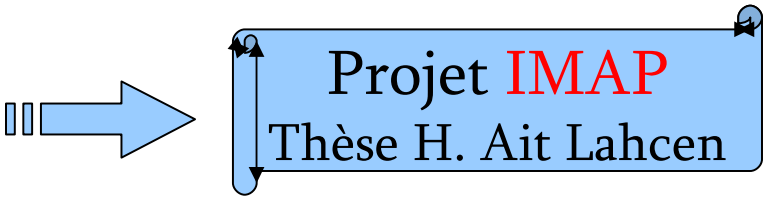
Conclusions

- Enseignements + (LAAS ==> ENSIB ==> INP)



Perspectives

- PolyOrBAC
  - Intégrité
  - Disponibilité
  - Systèmes distribués



- Q-ESP
  - Applications : avionique, VoIP, ...
  - Réseaux : NGN, MPLS, ...

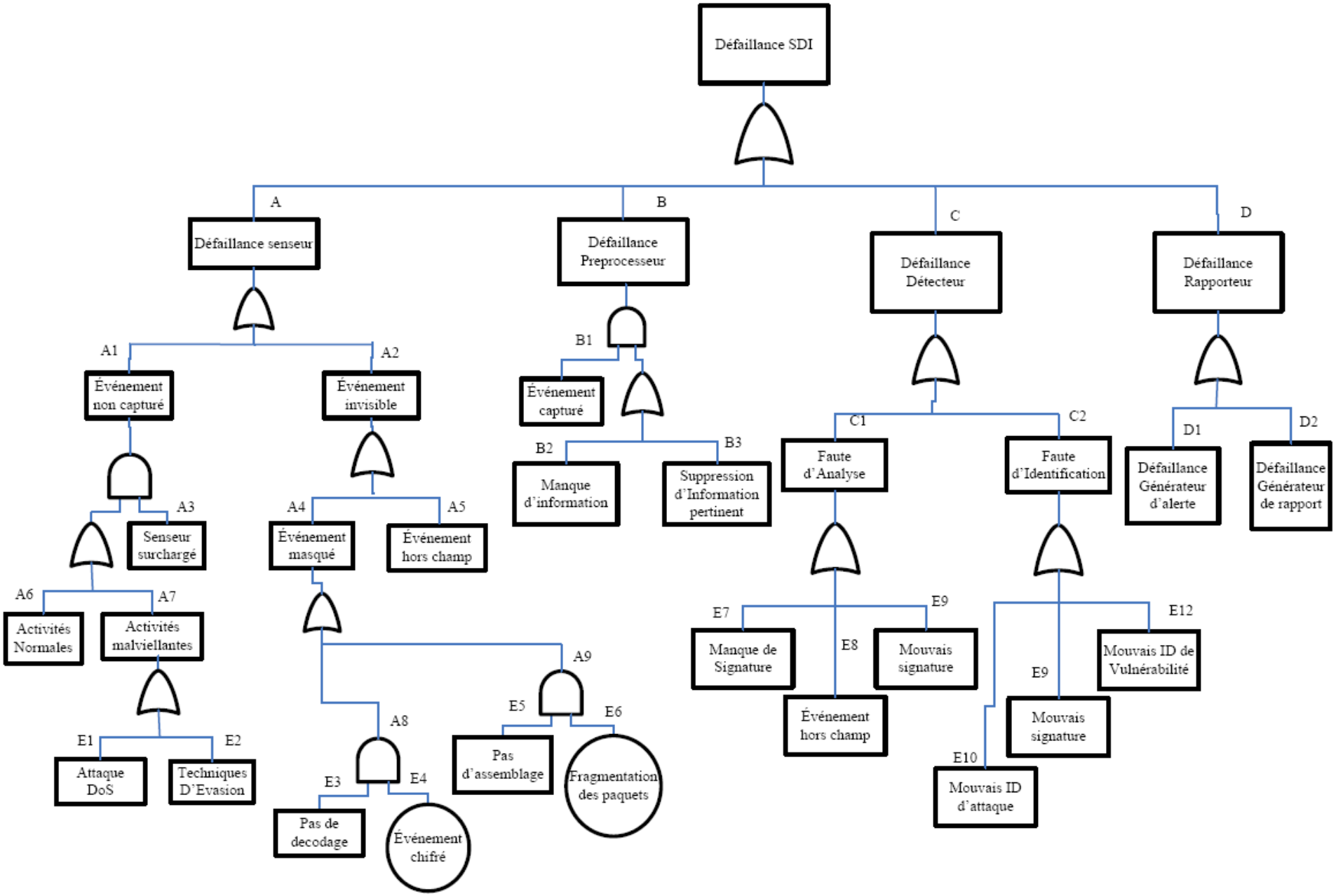
- Évaluation IDS
  - Contexte sans-fil ...

Merci

Questions

Evaluation des IDS

Sonde	Non capture des éventements intrusifs	Événements malicieux hors de la portée de la sonde. Evénements masqués	Intrusion non vue
		Suppression d'événements	Intrusions non vues ou vues partiellement
Pré-processeur	Suppression d'informations utiles	Format non approprié. Information insuffisante de la part de la sonde	Défaillance du détecteur
Détecteur	Non détection des événements intrusifs capturés	Défaillance du préprocesseur. Défaillance de l'algorithme de détection	Faux négatifs
	événements non intrusifs considérés comme intrusifs	Défaillance de l'algorithme de détection	Faux positifs
	Mauvaise identification		Rapport incorrect
Rapporteur	Alarme non générée	Mauvaise configuration	Faux négatifs


Défaillance SDI
A
Défaillance senseur
B
Défaillance Preprocesseur
C
Défaillance Détecteur
D
Défaillance Rapporteur
A1
Événement non capturé
A2
Événement invisible
A3
Senseur surchargé
A4
Événement masqué
A5
Événement hors champ
A6
Activités Normales
A7
Activités malviellantes
A8
A9
E1
Attaque DoS
E2
Techniques D'Evasion
E3
Pas de decodage
E4
Événement chifré
E5
Pas d'assemblage
E6
Fragmentation des paquets
B1
Événement capturé
B2
Manque d'information
B3
Suppression d'Information pertinent
C1
Faute d'Analyse
C2
Faute d'Identification
E7
Manque de Signature
E8
Événement hors champ
E9
Mouvais signature
E9
Mouvais signature
E10
Mouvais ID d'attaque
E12
Mouvais ID de Vulnérabilité
D1
Défaillance Générateur d'alerte
D2
Défaillance Générateur de rapport