Eléments de modélisation pour le test de politiques de sécurité

V. Darmaillacq, JC. Fernandez, R. Groz, L. Mounier, JL. Richier

Laboratoires LSR et VERIMAG - Institut IMAG - Grenoble

CRISIS 2005 - Vendredi 14 octobre 2005

Contexte du travail

Validation de la *mise en oeuvre* d'une *politique de sécurité* sur un système en *réseau ouvert*

⇒ Fournir des techniques et outils de **test** :

- destinés à des **administrateurs** réseau (ou **auditeurs** ...) ;
- prenant en compte une politique de sécurité **globale** ;
- utilisables sur un réseau **en exploitation**.

ACI 2004 "POTESTAT" (IRISA Landes et Vertecs, LSR, Vérimag)
Projet IMAG "MODESTE" (LSR, Vérimag)

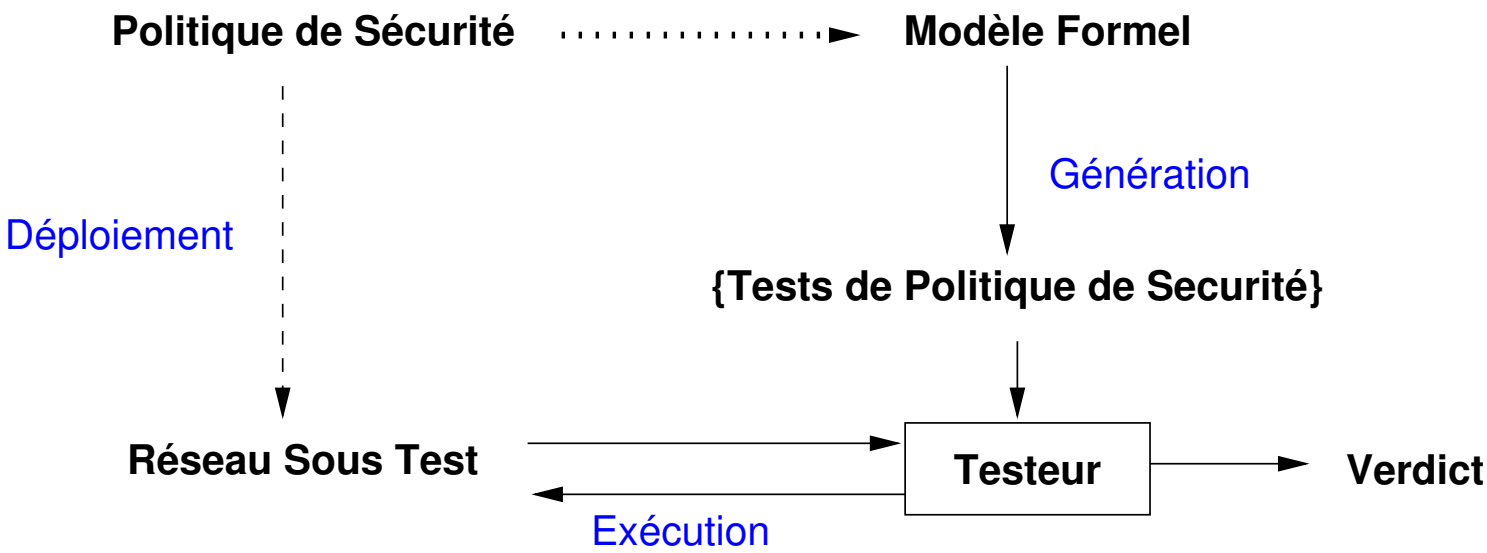
Approche proposée

Inspirée du **test de conformité** des protocoles :

$\Rightarrow$ "conformité" d'une implantation par rapport à une spécification ?

- basée sur des modèles formels :
  systèmes de transitions, machines à états
- relation de conformité entre modèles
- définition, génération et exécution de cas de tests :
  - séquences d'interactions testeur / implantation
  - délivrent un verdict $\in \{\text{Pass, Fail, Inconcl}\}$
- cadre standardisé, outils disponibles (académiques, commerciaux)

Application au test de politique de sécurité



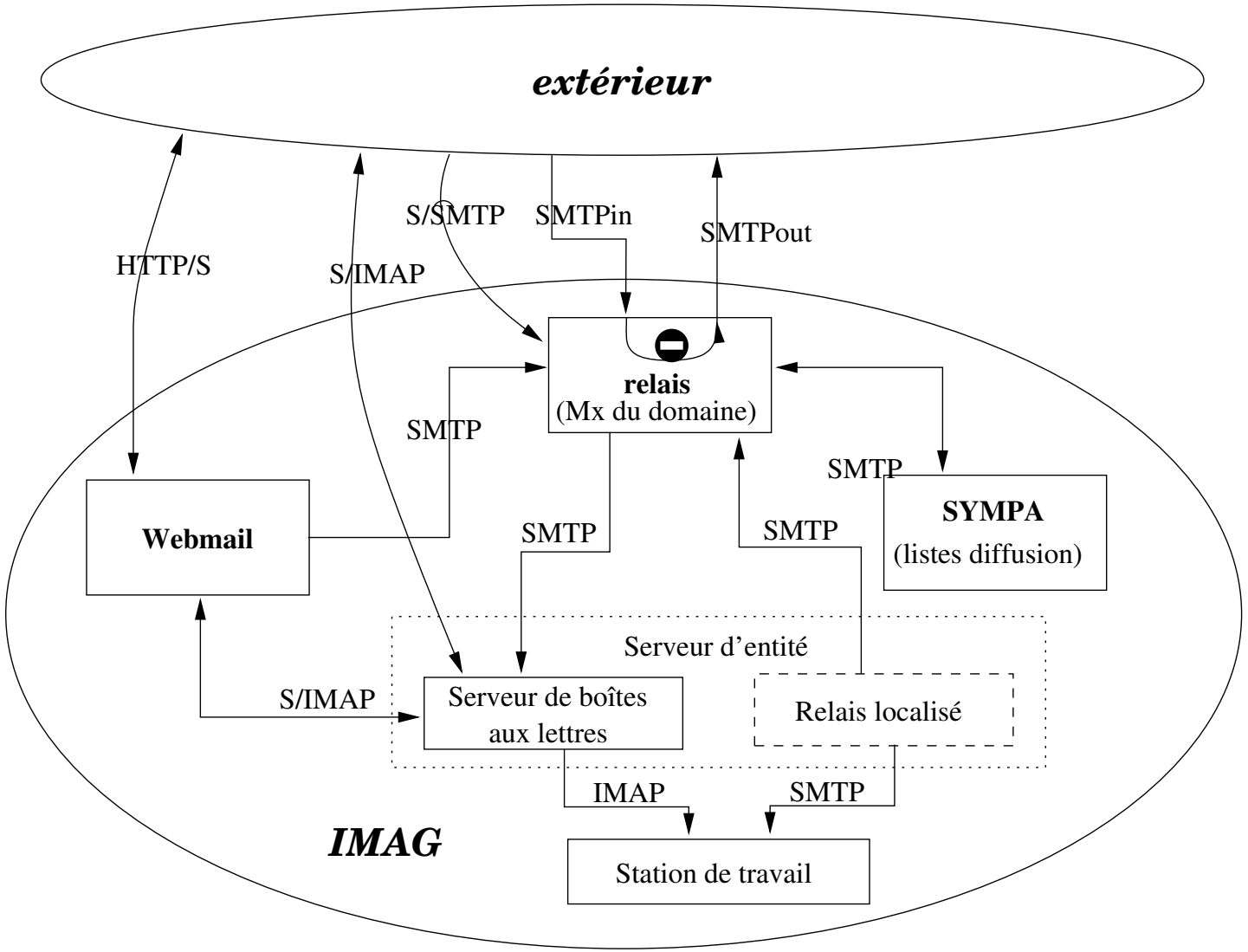
Deux questions :

- quels modèles formels pour les politiques de sécurité ?
- définition, génération et exécution de tests :
  $\Rightarrow$ que peut-on ré-utiliser du test de conformité ?

Plan

- Etude d'un exemple
- Du test de conformité au test de sécurité :
  les problèmes soulevés . . . et des éléments de réponse
- Conclusion et perspectives

Exemple : service de messagerie du réseau IMAG



Politique de sécurité (extrait)

	Règle
1	Les relais de messagerie ouverts sur l'extérieur doivent être placés dans la DMZ ; On les appelera par la suite "relais principaux".
2	Il n'y aura pas de compte utilisateur sur les relais principaux.
3	Les serveurs de boîtes aux lettres qui contiennent les comptes des utilisateurs seront dans la zone protégée.
4	Les relais principaux sont les seules machines habilitées au dialogue SMTP avec le monde extérieur : le relais du courrier entrant vers les serveurs de boîtes aux lettres et du courrier sortant vers l'extérieur s'effectue par les relais principaux.
5	Les serveurs de boîte aux lettres peuvent être utilisé comme relais internes de messagerie.
6	En entrée de site la politique de filtrage par défaut est que tout ce qui n'est pas explicitement autorisé est interdit.
7	Tous les messages de l'extérieur arrivant sur une machine qui n'est pas un relais principal doivent être redirigés sur un relais principal.
8	Il est interdit de relayer des courriers de l'extérieur vers l'extérieur.
9	[blacklisting] Refus de communiquer avec les relais appartenant à une liste donnée (quotidiennement mise à jour).
10	Des logiciels antivirus et antispams sont installés au niveau des relais de messagerie ou au niveau des boîtes aux lettres. Il est possible de mettre en place une protection au niveau des postes clients.
12	Toute pièce jointe à un courrier électronique doit être contrôlée par un logiciel anti-virus au moins une fois avant d'être ouverte (virus, troyens, malwares divers).
13	Tout courrier électronique doit être modifié s'il contient un virus. Le virus est supprimé du courrier et le destinataire en est prévenu.

Test d'une règle

Règle 5 : *"Les serveurs de boîte aux lettres peuvent être utilisés comme relais internes de messagerie"*

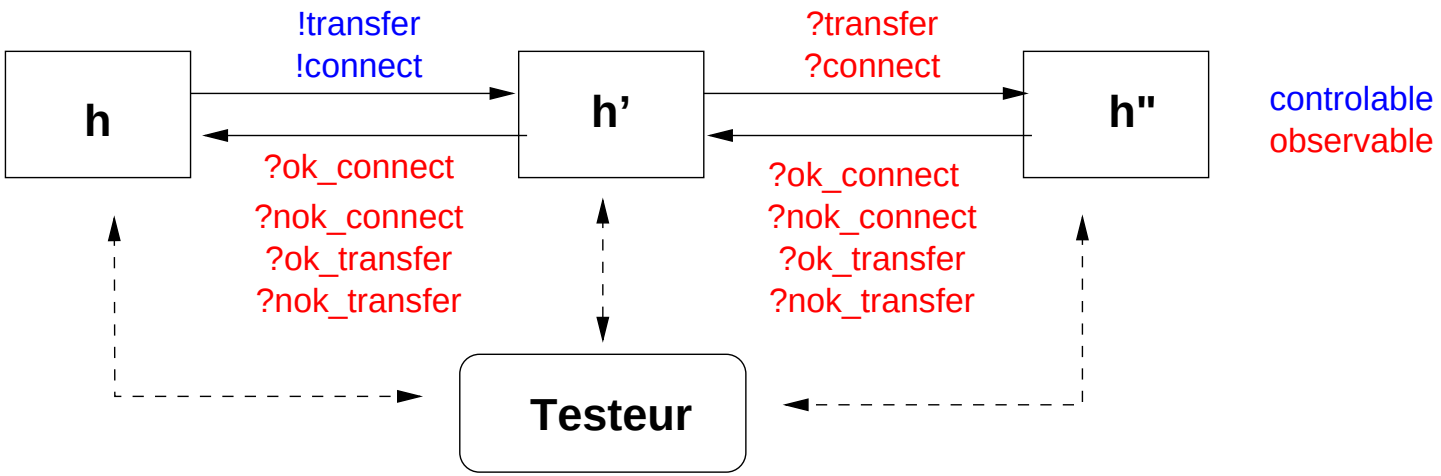
- Modalité de type **permission, autorisation** ($\Diamond$) :

$$\text{est\_serveur}(h') \Rightarrow \Diamond(\text{est\_relais}(h'))$$

- Test informel :
  1. choisir/installer une machine interne h (est_interne(h))
  2. envoyer depuis h un message m à une machine h' telle que :
     - h' est un serveur de boîte aux lettres (est_serveur(h'))
     - destinataire(m) $= h''$ avec est_interne(h'') et $h'' \neq h'$
  3. Verdict :
     - si m est relayé par h' vers h'' alors Pass sinon Fail
     - s'il y a échec dû à un problème réseau alors Inconcl

Architecture de test

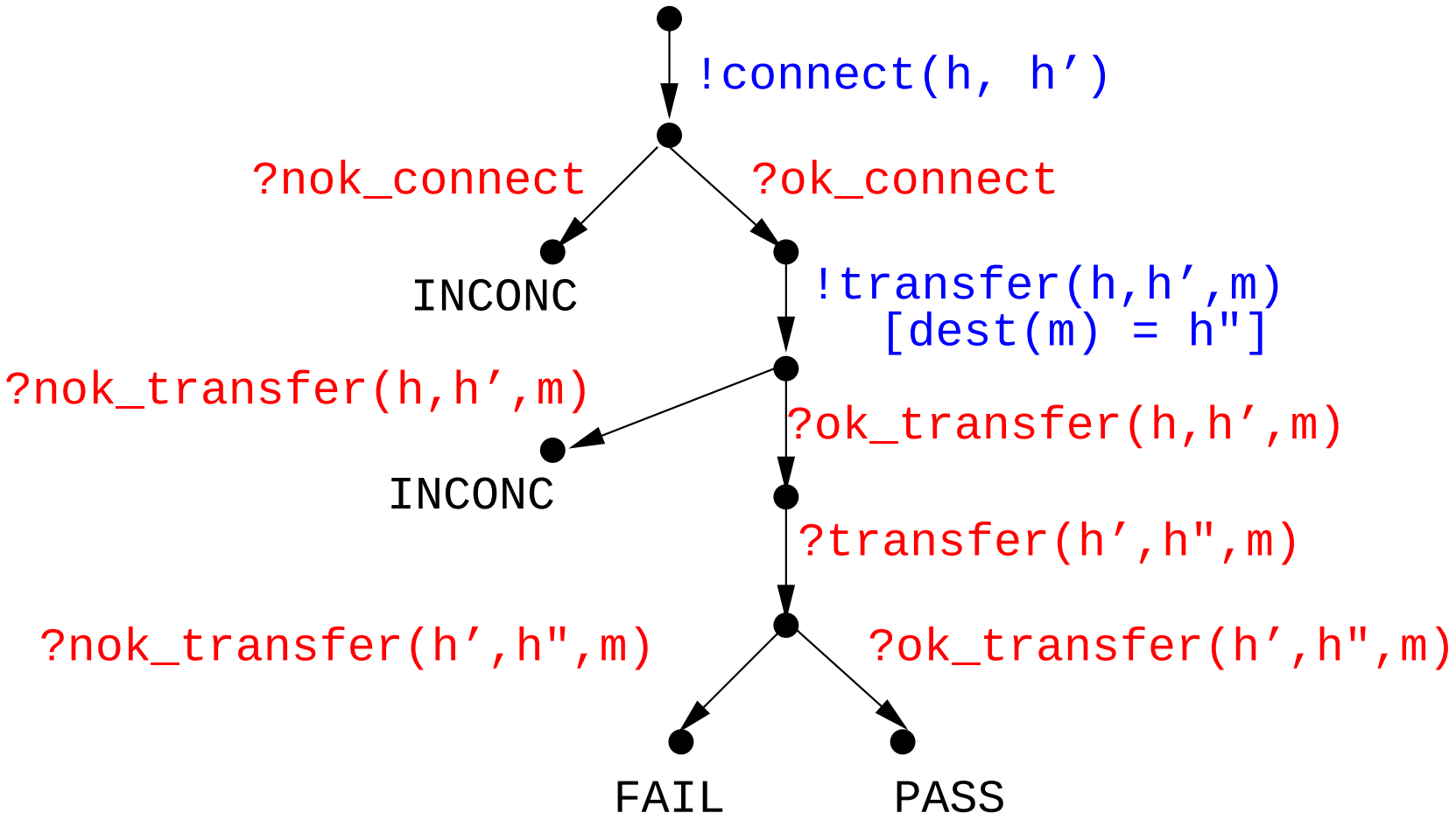
Envois de messages en 2 phases : connection ; transfert



Evénements pris en compte lors du test :

- demandes de connection, de transfert : `connect`, `transfer`
- réponses positives : `ok_connect`, `ok_transfer`
- réponses négatives : `nok_connect`, `nok_transfer`

Exemple de test abstrait (règle 5)



Problèmes spécifiques

(par rapport à du test de conformité classique)

- Tester des modalités spécifiques à la sécurité
- Hétérogénéité de l'architecture de test
- Structure et exécution des tests
- Concrétisation du test
- Fiabilité des informations recueillies
- etc.

Pb 1 : Modalités spécifiques à la sécurité

Définir un modèle formel pour les politiques de sécurité ?

- suffisamment expressif
- "compatible" avec les formalismes existants
  (Ponder, PDL, OrBAC, XACML, etc.)
  $\Rightarrow$ utilisation de modalités spécifiques :

permission ou autorisation, *obligation*, *interdiction* ...

- adapté à la validation par le test :

$\Rightarrow$ interprétation en terme d'états/transitions

Tester ces modalités ? (1)

Définir des séquences de test qui (in)-valident une propriété ?

permission, autorisation :

Un serveur de boîtes aux lettres peut être utilisé comme relais interne

- exhiber une séquence qui réalise le comportement attendu ;
- pas de verdict Fail (?) ; le verdict Pass est “sain” (*sound*).

Tester ces modalités ? (2)

obligation : (obligation conditionnelle)

toute pièce jointe à un courrier doit être controlée par un anti-virus

- exhiber une séquence qui contredit le comportement attendu ;
- le verdict Fail est "sain".

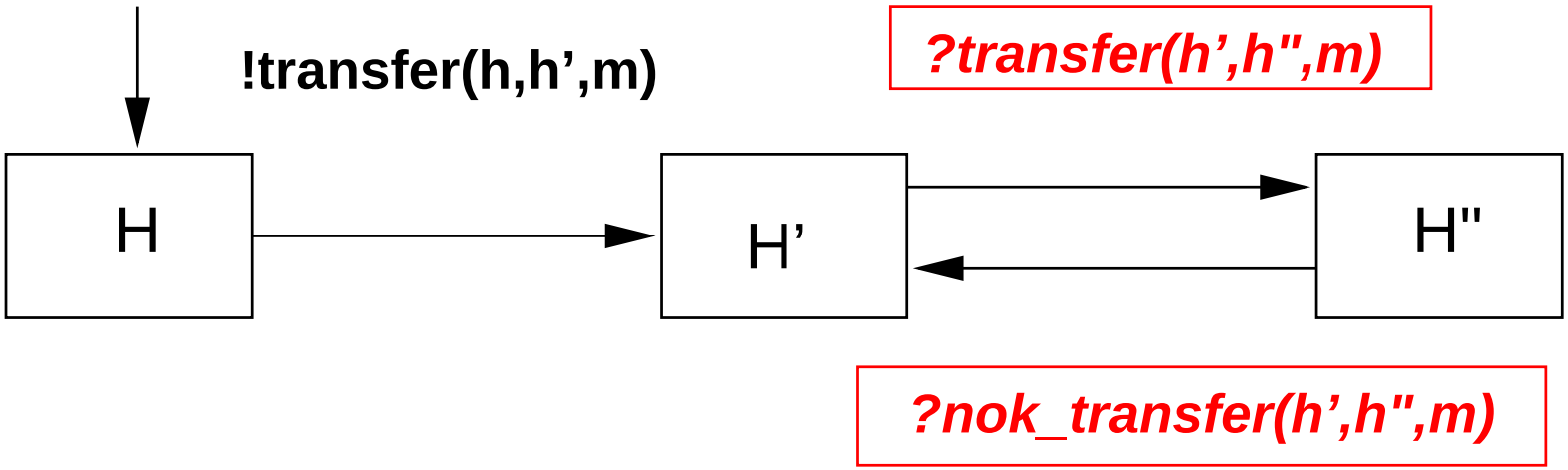
interdiction :

il est interdit de relayer des courriers de l'extérieur vers l'intérieur

- exhiber une séquence qui contredit le comportement attendu ;
- le verdict Fail est "sain".

Pb 2 : Hétérogénéité de l'architecture de test

Architecture de test pour la règle 5 :



- interaction avec différentes couches du réseau :
  $\longrightarrow$ application, système d'exploitation, protocoles, etc.
- informations disponibles (indirectement ?) sous différentes formes :
  $\longrightarrow$ sondes, journaux de bord, variables d'environnement, etc.

Pb 3 : Structure et exécution des tests

Test de conformité :

test actif : séquence / arbre d'*interactions* entre le testeur et l'implémentation.

test passif : exécution de l'implémentation sur une séquence donnée d'*entrées*, analyse des sorties obtenues (a posteriori, ou en ligne).

Test de politiques de sécurité :

Evénements non accessibles durant le test

- journaux de bord
- fichiers localisés sur des machines distantes, etc.

⇒ combinaison de tests actifs et passifs ?

Pb 4 : Concrétisation des tests

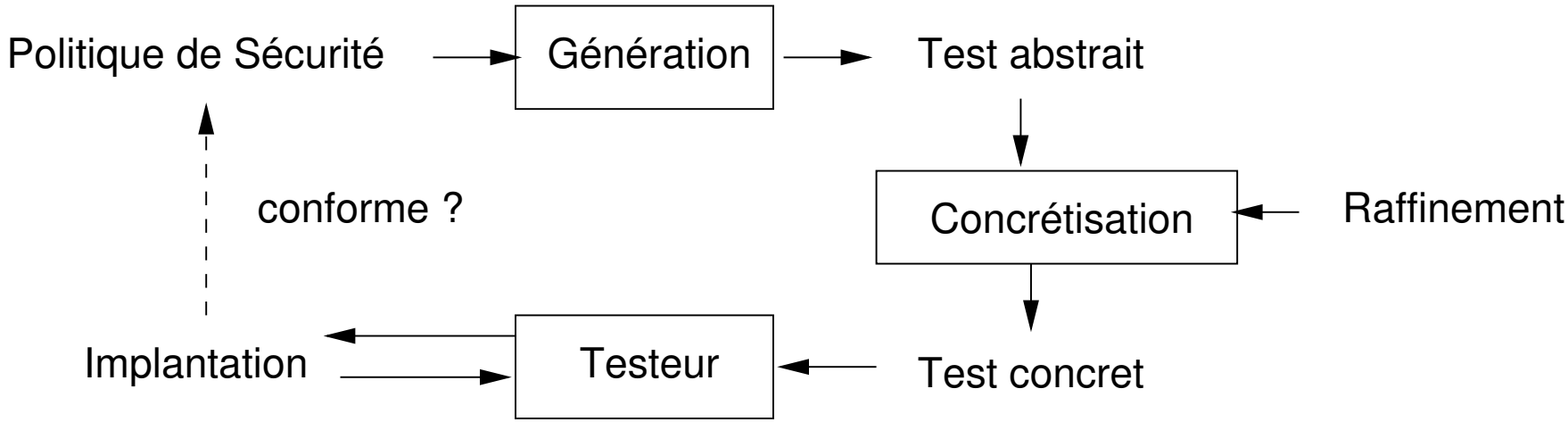
Différence de vocabulaire politique de sécurité / implantation :

politique : est_relais, est_interne, est_serveur, etc.

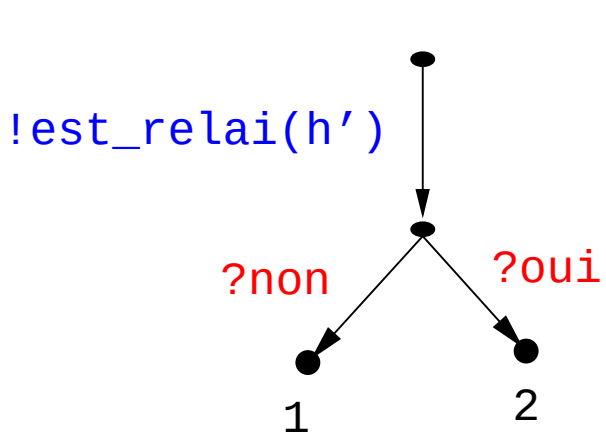
implantation : PDU, éléments de journal de bord, etc.

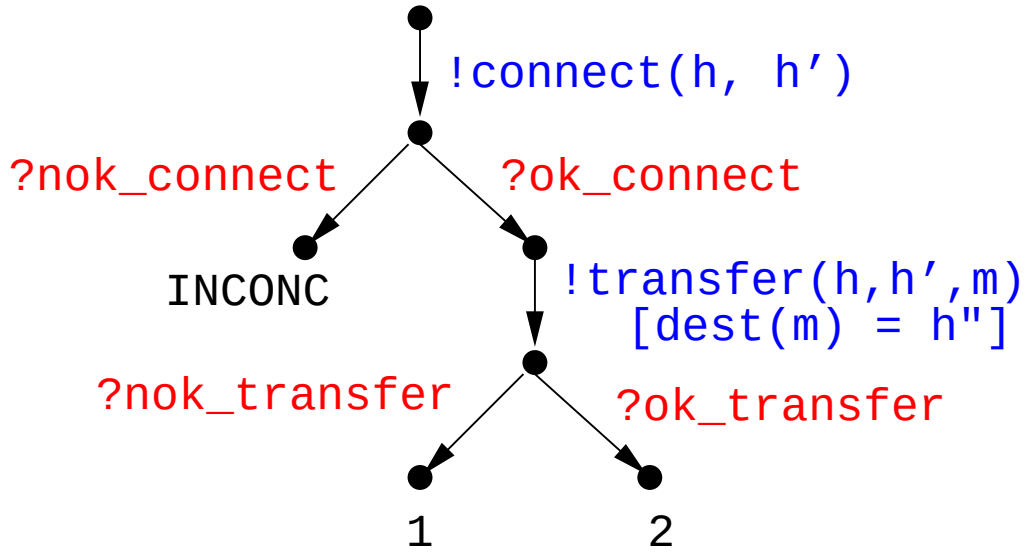
⇒ *concrétiser* les tests abstraits obtenus

⇒ définir une notion de *raffinement* d'un cas de test



Exemple





Raffinement d'un cas de test

Conclusion

- Test d'une politique de sécurité sur un réseau :
  définition, exécution, génération des tests
- Réflexion à partir d'un exemple : service de messagerie IMAG
- Comparaison avec le test de conformité :
  - architecture de test plus complexe
  - relation de conformité spécifique (modalités)
  - concrétisation des tests

Perspectives

Du point de vue du test :

⇒ prolonger des résultats théoriques existants :

- test *sous contexte*, raffinement de cas de test
- diagnosticabilité
- techniques de génération, etc.

Du point de vue de la sécurité :

⇒ définir des langages de description/spécification :

- politiques de sécurité
- éléments de réseaux, flux d'information, type de noeuds, ...

Poursuivre la réflexion sur des exemple ...