Politiques de Sécurité : éléments pour la modélisation et la génération de tests

Jean-Claude Fernandez

Laurent Mounier

Plan

- Objectifs
- Test : approche basée sur les modèles
- Modélisation
- exemple
- Relation entre la politique et l'implantation

Objectifs

- Formalisation
  - conformité par rapport à une politique de sécurité
  - “théorie du test” pour politiques de sécurité
- Mise en oeuvre
  - génération automatique de tests
  - exécution de tests
- Application à une étude de cas

Problèmes abordés

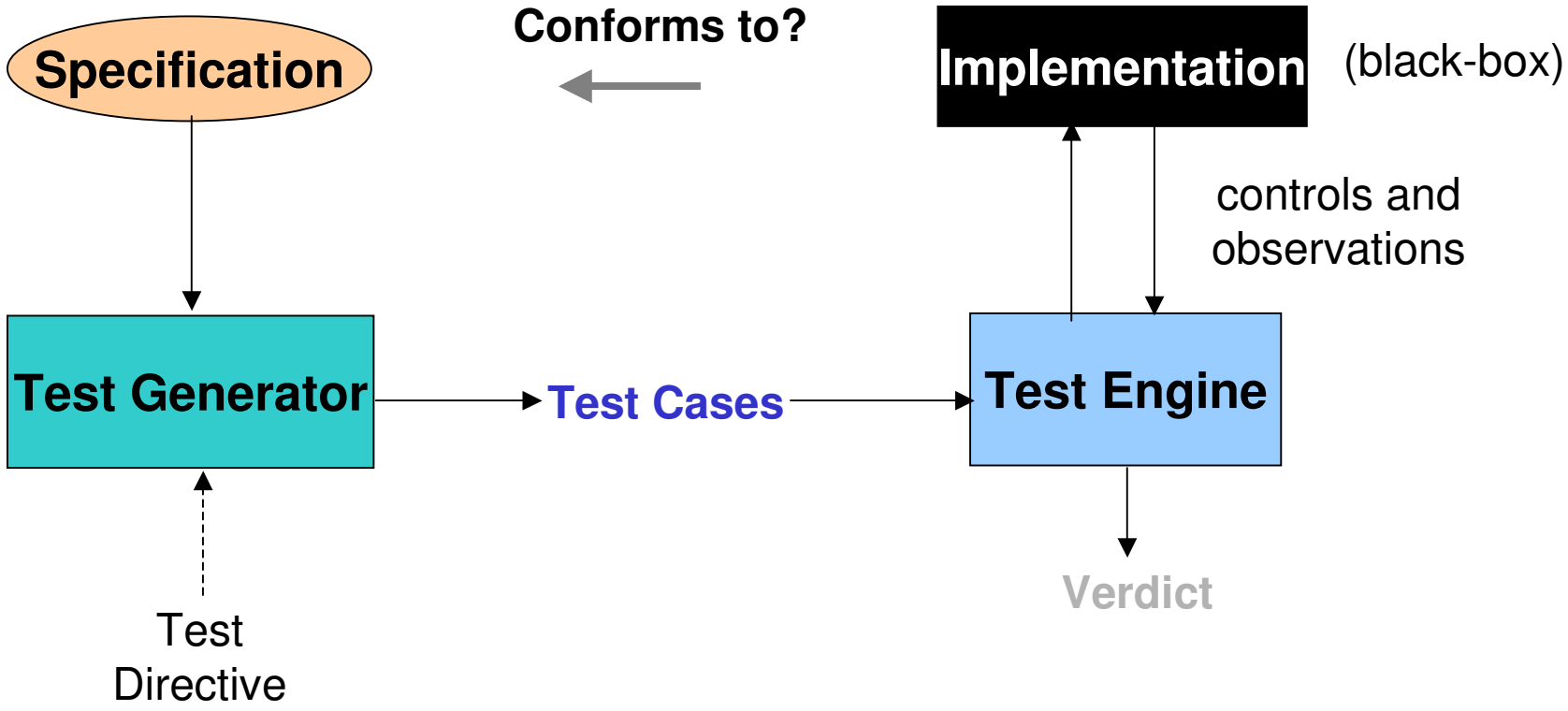
- Modélisation de politiques de sécurité
- Formaliser la notion de test,

  test de programmes, test “orienté propriété”

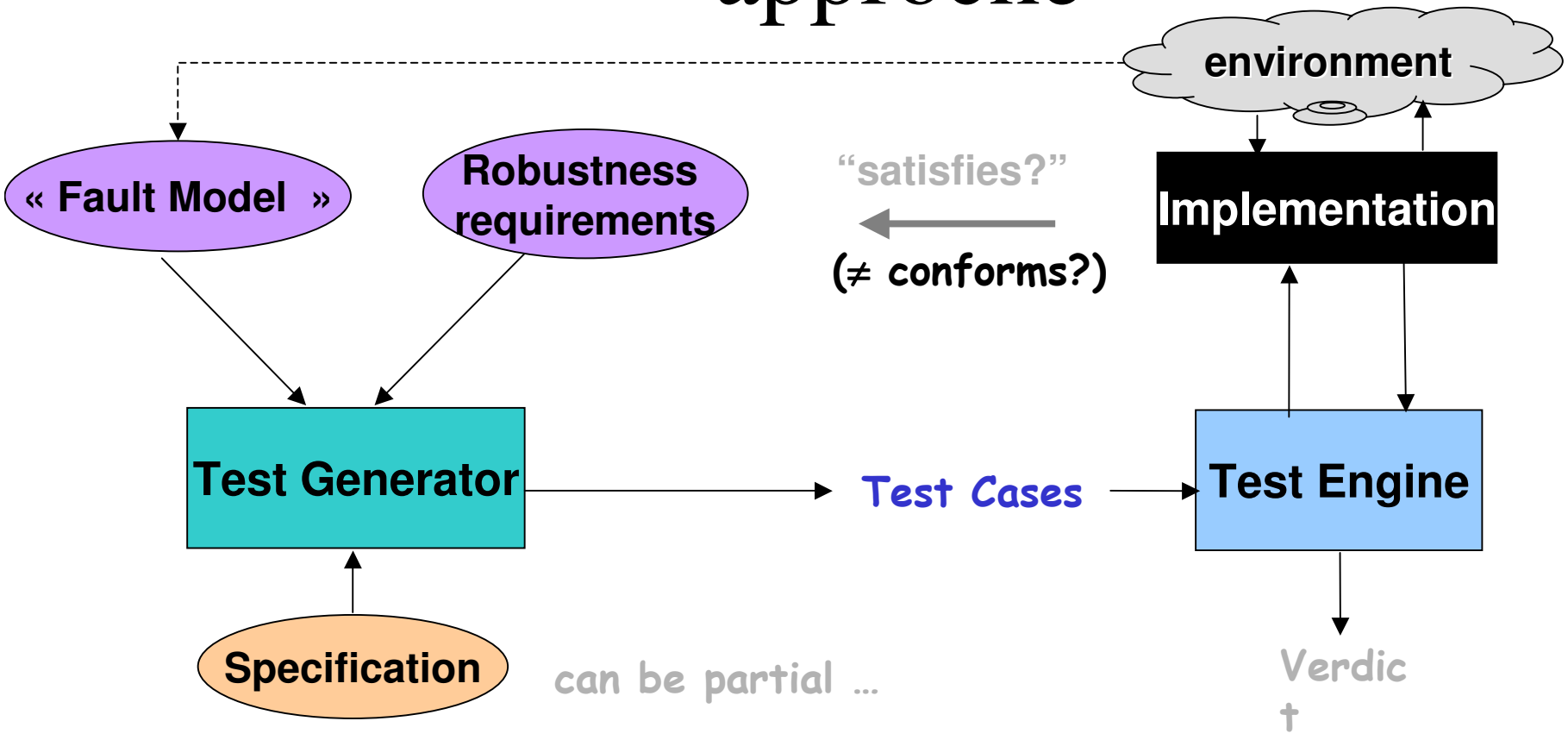
  (interactions avec le testeur , verdicts, …)
- Algorithmes de génération
- Instrumentation de code / monitoring

Background: (black-box) *conformance testing*

conformance testing: check if an implementation conforms to a given specification

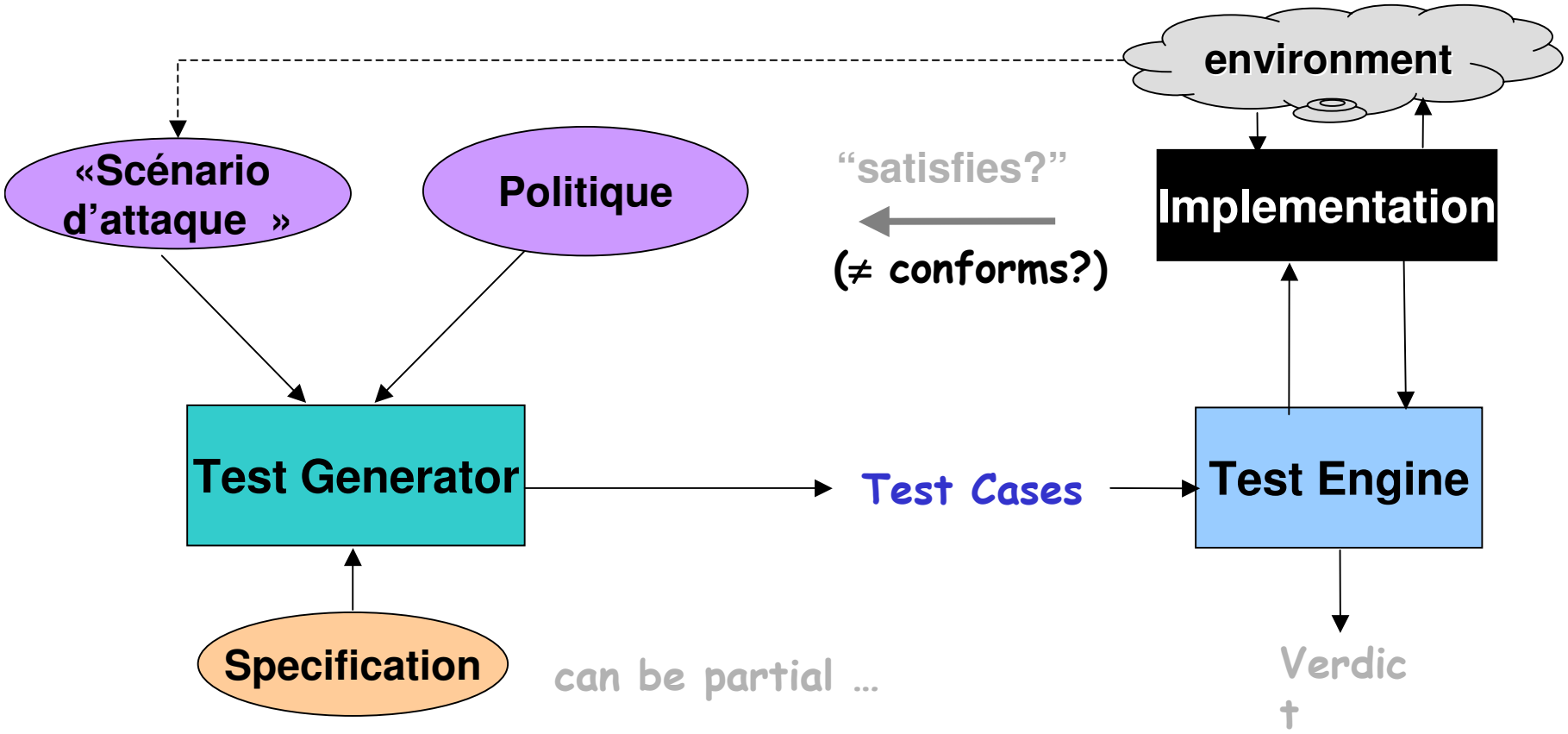


Test de Robustesse : une approche



⇒ model-based approach, inspired from the conformance testing framework

Test de Politiques de sécurité



Modèles

Spécifications IF:

- processus = LTS + variables +horloges
- communications : asynchrone, canaux fiables/non fiables, bornés/non bornés, …
- variables partagées

Modèles de faute : mutations

- Annotations sur la syntaxe

Propriétés de robustesse

Logiques temporelles

Automates de Rabin

Une séquence d'exécution est acceptée ssi elle passe
infiniment souvent par un ensemble d'états L et
non infiniment souvent par un ensemble d'états U

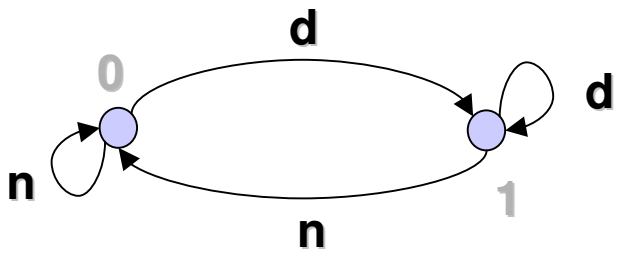
Automates de Rabin paramétrés

Des bornes sont associées aux états de L et de U

Exemple

L = {1}

U = {0}



Accepted traces:

RA: $(d+n)^*.d^\omega$

PRA: $(d+n)^i.d^j$, with $i< c_u$ and $j>c_l$

Modélisation des politiques de sécurité

- Automates + extensions
  - Variables
  - États distingués
- Définis sur un vocabulaire abstrait
- Relation avec les modalités employés dans les formalismes liés à la sécurité ?

Exemple

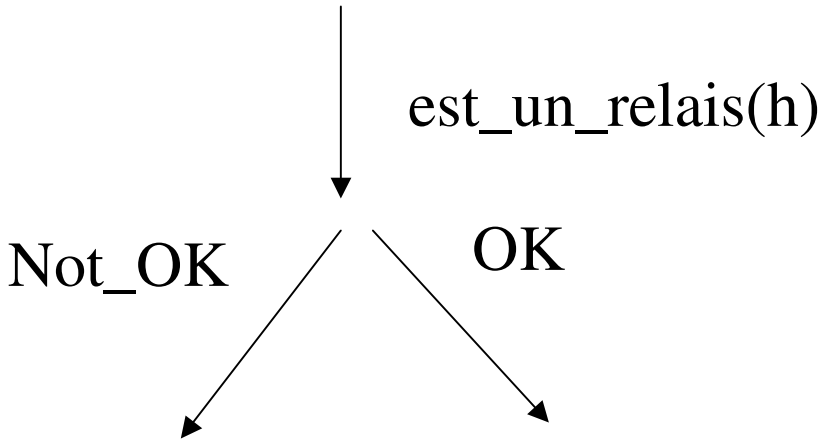
Flux de trafic autorisés liés au courrier électronique

Par rapport au réseau

- Une machine peut être interne / externe
- Machines accessibles de l'extérieur, ou non
- Une machine peut être une station, un serveur de boite aux lettres, ou un relais

Exemple de politique

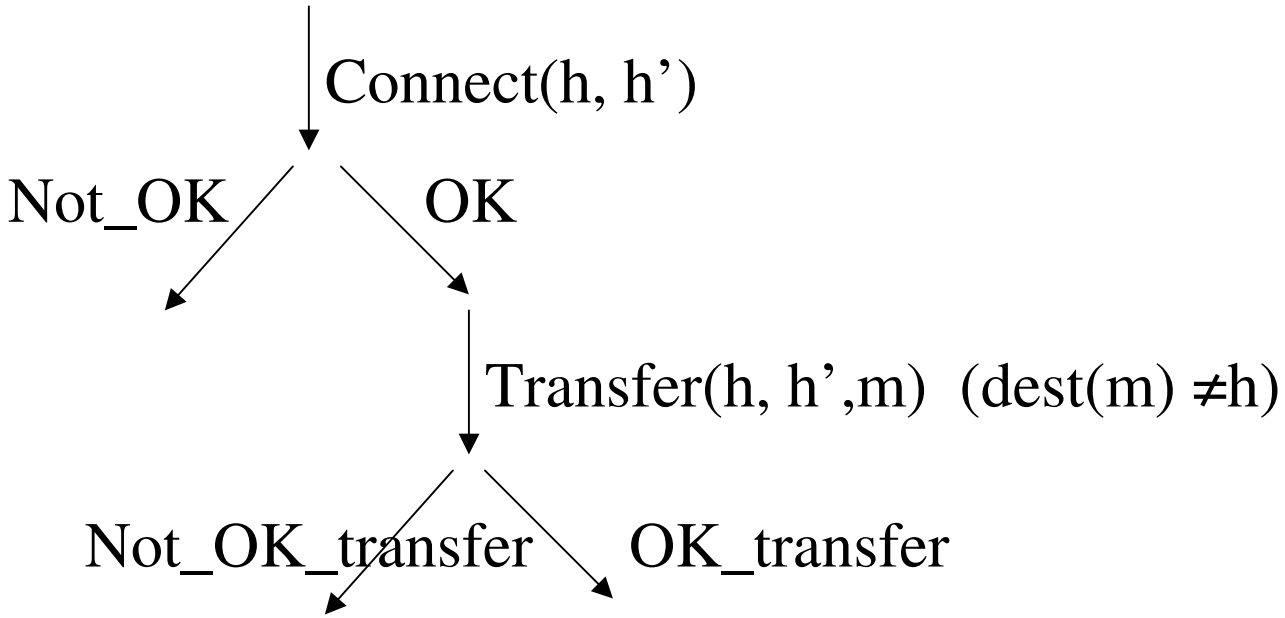
Pour une machine h, le prédicat « être un relais » peut être exprimé par l'automate suivant :



Politique et implantation

- Différence de niveau d'abstraction entre la politique et l'implantation effective
- Une action de niveau abstrait peut être exprimée au niveau de l'implantation par des séquences, des arbres voire des automates
- Nécessité de définir une correspondance entre les vocabulaires

Exemple


Connect(h, h')
Not_OK
OK
Transfer(h, h',m) (dest(m) ≠h)
Not_OK_transfer
OK_transfer

Exemple

- On associe à l'action est_un_relais, la séquence exprimant une demande de connexion, suivie d'un acquittement, et une demande de transfert suivie d'un acquittement

Relation entre politique et implantation : le cadre

- Définition d'un mapping entre une politique de sécurité et une implantation ;
- La politique de sécurité et l'implantation sont représentées par des automates, un abstrait et un concret
- La satisfaction de la politique de sécurité revient à mettre en correspondance l'automate abstrait et l'automate concret