POTESTAT

LSR
IMAG

POlitiques de sécurité: TEST et Analyse par le Test de systèmes en réseau ouvert

LSR-IRISA-VÉRIMAG

ACI Sécurité Informatique – Toulouse 15-17/11/2004
Projet 2004

IRISA

Vous avez dit politique de sécurité ?

LSR
IMAG

- Sens 1: politique de sécurité d'un SI & d'un réseau
  - traduction concrète: charte d'utilisation, règles de configuration de serveurs, de routeurs...
- Sens 2: politique de sécurité d'un système fermé sûr (C.C.) certifiable (ex. carte à puce)
  - traduction concrète: cahier des charges type CC
- Sens 3: politique de sécurité « O/S » ou d'exécution de pgm (ex. Java, mécanismes JVM + bibliothèques)
- ...

POTESTAT cherche à aborder les trois

IRISA

Point de départ - thème

LSR
IMAG

Intersection de 3 problématiques-compétences

- Politiques de sécurité sur logiciels en réseau
  - savoir-faire, architecture intégrant des solutions
  - organisation, principes
- Modélisation formelle (Génie Logiciel)
  - moyen de description et de calcul
  - base pour test (et vérification etc.)
- Test
  - comme moyen de renforcer la confiance/système

IRISA

Pourquoi le test ?

LSR
IMAG

- Etat de l'art
  - analyse formelle de systèmes de confiances réduits (carte à puce...)
  - modèles de détection a posteriori ou en ligne (intrusion, analyse de trafic...)

  Pb: complexité des systèmes en réseau, échelle et multiplicité des niveaux
- Le test est une réponse classique pour:
  - augmenter la confiance
  - échantillonner / complexité
  - confronter au syst. réel

IRISA

Du test au « test à base formelle »

LSR
IMAG

- Méthodes/travaux existants ~test
  - Check-list (auditeurs, administrateurs):
    - sondes sur points isolés
  - Analyse statique de code / propriétés de sécu.
    - preuve partielle - complémentarité /test
- Objectif de POTESTAT
  - avoir un modèle formel intégré (+- complet) d'une politique de sécurité
  - en déduire des tests de la conformité d'un système à cette politique

    => Test de conformité implém/spéc

IRISA

Méthodes de test pour qui ?

LSR
IMAG

- 1- Auditeurs&administrateurs de SI&réseaux
  - automatiser la vérification de conformité/politique:
    - cohérence des choix faits pour le respect des propriétés de sécurité (test supplée vérification)
    - rattraper les erreurs de configuration
- 2- Concepteurs de systèmes sûrs & auditeurs
  - outils d'analyse du système embarqué
- 3- Téléchargement de code
  - test de scénarios d'attaque déduits du modèle

IRISA

LSR
IMAG

Problèmes étudiés (1)

- **Modélisation du système** (réseau/applet)
  - Eventuellement acquisition de modèle par analyse statique de code (flot de contrôle et de données), ou de configuration du réseau
  - Prise en compte des mécanismes de défense
- **Modélisation des politiques de sécurité**
  - Automates à la Schneider _ étendus par données
  - Ponder, PDL, OrBAC...
  - Description à plusieurs niveaux, relations entre niveaux, par ex:

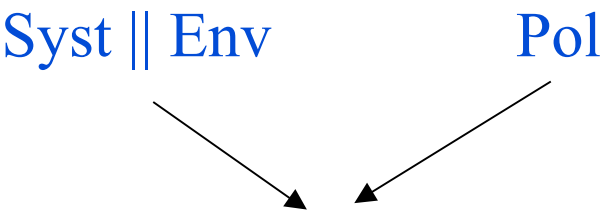
Organisationnel	Restrictive: tout interdit sauf mél et web
Mise en œuvre	Interdire les ports sauf 80 et 25
Technique	Règles de filtrage des pare-feux

IRISA

Problèmes étudiés (2)

LSR
IMAG

- **Formalisation de la conformité/politique**
  - Test de conformité: s'appuie sur une relation de conformité, critère de décision testable du respect de la politique
  - Approche multi-niveaux: tester la conformité
    - mise en œuvre / organisationnel (modèle/propriétés)
    - technique / mise en œuvre (config réelle/modèle)
- **Utilisation de la relation de conformité: pour déduire le test du modèle formel**
  - Test de sécurité: attaque



Problème : synthétiser Att tq ¬ (Syst || Att **confsec** Pol)

IRISA

Problèmes étudiés (3)

LSR
IMAG

- **Sélection hors-ligne** (sur les modèles)
  - de scénarios d'attaques
  - oracle de violation de la sécurité

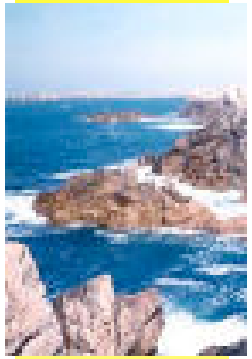
  S'appuie sur des techniques de synthèse de contrôleur/génération de tests

  Abstraction et indécidabilité
  approximations fausses attaques
- **Test en ligne** (sur le système réel)
  - Contrôle: guidage par les attaques
  - Observation : vérification de violation par l'oracle

IRISA

Ecueils possibles (test vs sécu)

LSR
IMAG



- Canaux cachés: vérification (et donc test) illusoire ?
- La notion de propriétés de sécurité est-elle pertinente pour le test ?
- Check-list antinomique de modèle
- Les responsables de sécu font confiance à l'expérience, à l'échange d'info, à l'organisation et à la métrologie

IRISA

Participants au projet

LSR
IMAG

- IRISA
  - Thierry Jéron, Hervé Marchand, Vlad Rusu (VERTECS)
  - Thomas Jensen, Arnaud Gotlieb (LANDE)
- LSR - équipe Vasco
  - Roland Groz (coordinateur), Jean-Luc Richier
  - Vianney Darmaillacq (doctorant)
- VÉRIMAG - équipe DCS (Syst.Distrib. complexes)
  - Jean-Claude Fernandez, Yassine Lakhnech, Laurent Mounier
  - Cyril Pachon (doctorant)

IRISA

Compétences des équipes

LSR
IMAG

Modèles et techniques de vérification&test
(model checking, interprétation abstraite, preuve)
pour syst. distribués/réactifs/temps-réel

- génération de tests de conformité /objectif de test
- synthèse de contrôleurs /objectif de contrôle
  vérification en ligne (run-time)

Modèles : automates et systèmes de transition,
étendus avec variables (commandes gardées)

Techniques : model-checking, preuve, analyses statiques,
interprétation abstraite, résolution de contraintes.

Outils : Plate-forme IF, test (TGV, STG), contrôle (Sigali),
IA (NBAC)

IRISA

Compétences / sécurité

LSR
IMAG

- Analyse statique et vérification pour la sécurité logicielle.
  - Code mobile Java (inspection de la pile)
  - Carte à puces (Java Card)
  - Disponibilité des services de composants
- Test structurel par résolution de contraintes.
  - Modèles logiques et probabilistes
  - Application à Java Card
- Model-checking /certification carte à puce
- Sécurité opérationnelle des réseaux

IRISA

Des questions ?

LSR
IMAG

IRISA

Nos questions pour l'ACI (pour vous!)

LSR
IMAG

- Modèles pour les politiques de sécurité, largeur de spectre
  - formalismes émergents ?
- Propriétés de sécurité: formalisation, spécificités sémantiques
  - beaucoup de propriétés (même la disponibilité bornée) sont des propriétés de sûreté (PAS de SdF!) i.e. violables sur des traces finies
- Complémentarité du test / autres approches

IRISA