ACI Sécurité & Informatique

Projet POTESTAT

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

Security policies: test directed analysis of open network systems

Présentation

Ce projet est financé dans le cadre des ACI Sécurité pour une durée de 3 ans (septembre 2004 - septembre 2007).

Thème du projet

POTESTAT se situe à l'intersection de techniques et de problématiques de recherches.

- les politiques de sécurité s'appliquant sur des logiciels en réseau
- la modélisation formelle
- le test comme moyen d'établir la confiance dans des systèmes

POTESTAT s'intéresse donc à une modélisation formelle de politiques de sécurité pour des réseaux et des logiciels communicants. Sur cette modélisation formelle, on peut alors appuyer des approches de test bien outillées et automatiques. Le test est une technique complémentaire des analyses qui peuvent être menées avec des outils de vérification

- parce que la complexité des systèmes et même simplement de leurs modèles rend en général impossible une vérification complète, elle doit donc être complétée par des tests prolongeant l'analyse sur des scénarios plus complexes
- le test, même s'il est dérivé du modèle, pourra être effectué sur le système réellement en opération, et non pas sur une analyse d'un modèle antérieur.

Equipes participantes

- LSR/IMAG - INPG, Equipe Vasco
- VERIMAG, Equipe DCS
- IRISA, Equipe Vertecs
- IRISA, Equipe Lande
- IRISA Equipe DistribCom

Coordinateur du projet

Roland Groz (LSR/IMAG), courriel: Roland.Groz@imag.fr

Site externe

http://www-lsr.imag.fr/POTESTAT/

Résumé du projet POTESTAT

Dans le cadre de la réalisation de services de plus en plus ouverts, s'appuyant sur la mise en réseau de parties de systèmes informatiques, avec des solutions hétérogènes, les responsables de la sécurité manquent souvent d'éléments d'analyse bien formalisés. La sécurité de ces systèmes est donc organisée en fonction de connaissances pragmatiques, en s'appuyant sur des failles connues et les mesures de protections associées. Il reste alors à vérifier que la politique de sécurité ainsi définie est bien celle qui est effectivement mise en oeuvre dans le système. Pour cela, on procède généralement à des audits, qui portent sur les procédures administratives et sur la configuration du systèmes. Des tests sont ensuites menés, correspondant à des sondages du système, pour vérifier si certaines vulnérabilités connues ne resteraient pas présentes.

S'il existe des outils pour certains tests spécifiques (comme les craqueurs de mots de passe), il n'y a pas de solution analysant la conformité globale d'un système par rapport à une politique de sécurité. Plusieurs raisons peuvent expliquer ces déficiences.

D'abord, il y a peu d'études actuellement sur la modélisation formelle complète de politiques de sécurité, même si certains aspects, comme le contrôle d'accès, ont fait l'objet d'études plus poussées. Ensuite, les travaux d'analyse par vérification menés en sécurité ont plus souvent porté sur la vérification d'éléments ponctuels, comme les protocoles cryptographiques ou l'analyse de code. Enfin, la plupart des travaux menés concernent la vérification a priori de la cohérence de politiques de sécurité, avant leur mise en oeuvre. Nous nous intéressons ici au test de la conformité de la configuration de systèmes par rapport à une politique définie.

Dans le cadre du projet POTESTAT nous envisageons d'aborder le problème du test de politique de sécurité sur un réseau ouvert selon les points suivants :

- Modélisation formelle adéquate pour les politiques de sécurité, permettant une analyse par le test.
- Définition d'une notion de conformité de la configuration de systèmes par rapport à ces éléments d'une politique de sécurité. L'objectif est de parvenir à une théorie du test analogue à ce qui peut exister dans le domaine des tests de protocoles (Z.500).
- Méthodes de test de la conformité à une politique, avec en particulier les problèmes de testabilité, d'environnement d'exécution, d'analyse de code et de sélection de tests pertinents.

L'objectif ultime (à plus long terme que le travail théorique de l'ACI) est que les responsables de sécurité des outils d'analyse puissent disposer d'outils, permettant :

- de modéliser les flux d'informations, les éléments du réseau (protocoles utilisés, types de noeuds et type de sécurité associée etc.), afin de pouvoir décrire plus formellement la politique de sécurité dans l'optique d'un test de conformité
- d'outiller cette modélisation afin de pouvoir mener des vérifications de cohérence ou des recherches de point faible
- d'étudier plus particulièrement une automatisation des procédures de test des systèmes pour vérifier si la politique de sécurité effectivement mise en oeuvre correspond bien à celle déclarée.