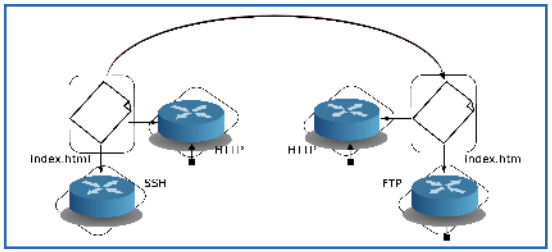
Prévision d'incidents avec Net Qi

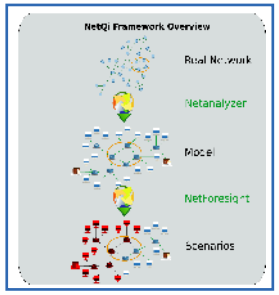
Avant de détecter des intrusions, il est utile de savoir prévoir les pannes et les attaques contre un réseau donné.

Net Qi est une architecture, en cours de développement, permettant l'analyse des points faibles d'un réseau.

- Net Analyzer : un outil reconstruisant les dépendances entre services, et entre fichiers et services, à partir d'une analyse statistique des flux réseau ;
- Net Foresight : vérification de propriétés de robustesse et en général de résilience des réseaux face aux pannes et aux attaques. Ceci est fondé sur des techniques de model-checking de la logique TATL ♦ sur des jeux d'automates temporels.



Un graphe de dépendances d'un serveur Web redondant simple. Le fichier index.html de droite est copié sur le serveur de gauche à intervalles réguliers. Si l'administrateur peut patcher les services vulnérables assez vite, cette architecture garantit un temps minimum en ligne ("service level agreement"). Sinon, tout le réseau peut devenir compromis.



NetQi est composé d'un logiciel de capture des dépendances entre services et fichiers sur le réseau à analyser (NetAnalyzer), et d'un outil d'analyse de l'impact de ces dépendances sur la vulnérabilité du réseau (NetForesight).

SECSI *(Sécurité des Systèmes d'Information)* a pour spécialité la **vérification** automatique de propriétés de **sécurité** de systèmes et réseaux informatiques. SECSI se fonde pour ceci essentiellement sur des outils venant de la **logique** (logiques, model-checking, automates).

SECSI s'intéresse notamment à :

- la vérification automatique de protocoles cryptographiques ;
- la détection d'intrusions (cette démo) ;
- l'analyse statique de code pour la sécurité.

$$\langle\!\langle A \rangle\!\rangle \blacksquare x \cdot \neg \Diamond_{=} \mathrm{Avail} \Rightarrow [\ \langle\!\langle A \rangle\!\rangle \blacklozenge y \cdot y \leq x + 5\ \mathrm{s}. \wedge \langle\!\langle A \rangle\!\rangle \blacksquare z \cdot z \leq y + 1\ \mathrm{month} \Rightarrow \Diamond_{=} \mathrm{Avail}]$$

SECSI utilise différentes logiques appliquées à la sécurité : ici, une formule de TATL♦ exprimant la propriété de "service level agreement" d'un réseau.

L'équipe-projet SECSI est commune avec le LSV (CNRS et ENS Cachan), localisée à Cachan.

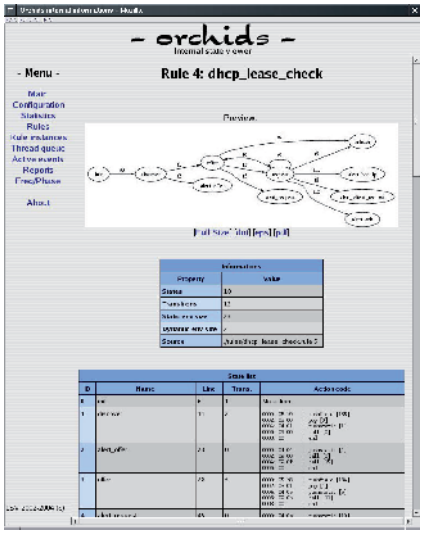
Équipe-projet SECSI

Centre de recherche INRIA Futurs

Laboratoire LSV
ENS Cachan
61, avenue du président Wilson
94230 Cachan

Jean Goubault-Larrecq

http://www.lsv.ens-cachan.fr/~goubault/



INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

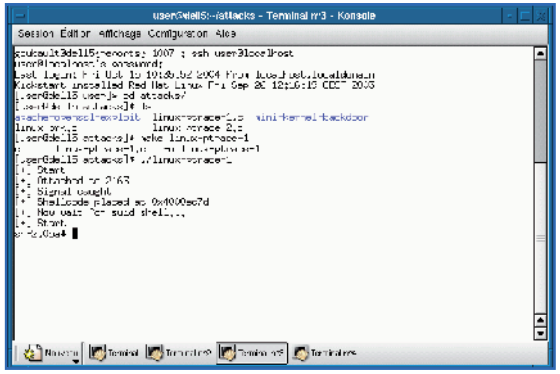
INRIA

Détection d'intrusions ORCHIDS + Net QI

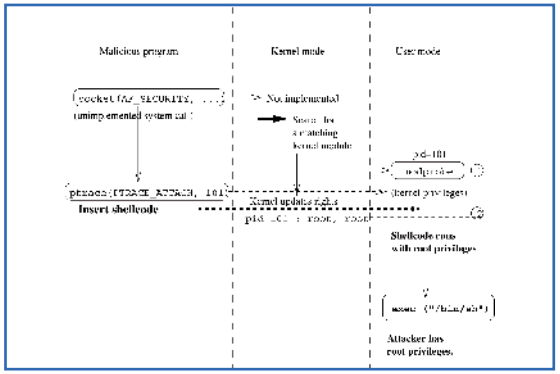
Détection d'intrusions complexes avec ORCHIDS

Les attaques contre les systèmes d'exploitation et les réseaux deviennent de plus en plus complexes, et difficiles à détecter et à contrer. Ceci tient notamment au fait qu'elles se font en plusieurs étapes. ORCHIDS les détecte en reconnaissant en temps réel les suites d'événements caractéristiques de ces attaques, via des signatures.

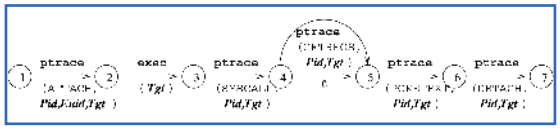
On notera qu'une seule signature ORCHIDS est capable, plus généralement, de détecter toute une famille d'attaques. ORCHIDS peut même détecter et contrer certaines attaques "zéro-day".



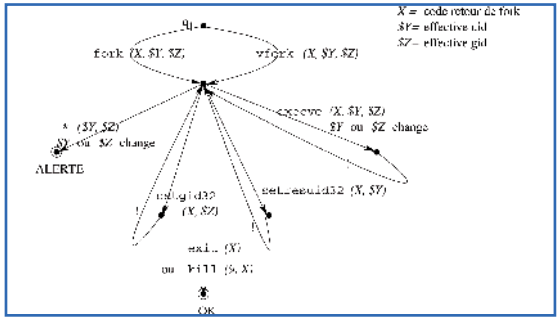
L'attaque ptrace de 2003. L'intrus a initialement un compte sur la machine cible. Il gagne les droits du super utilisateur (root). Ceci est matérialisé par le signe **'#'** sur la dernière ligne.



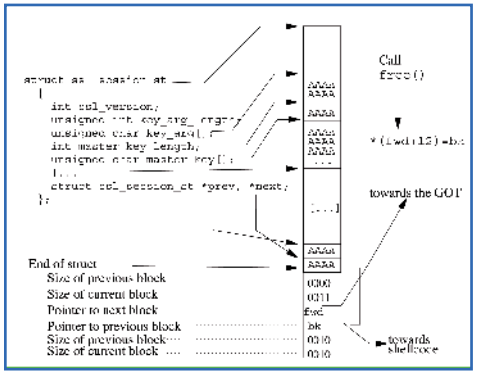
Le principe de l'attaque ptrace de 2003.



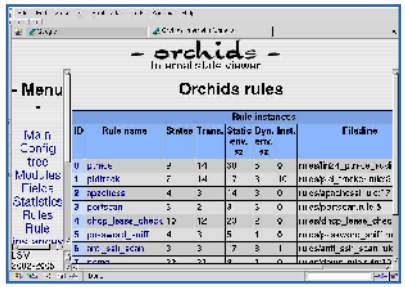
Une représentation graphique d'un automate détectant l'attaque ptrace.



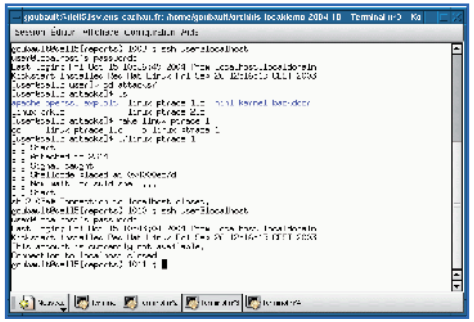
L'attaque do_brk de 2005 a été responsable de la mise hors ligne des serveurs maîtres GNU et Debian. Elle est indétectable au sens où elle ne produit aucun événement observable.
ORCHIDS détecte la corruption qui s'ensuit grâce à un moniteur (ci-dessus), et lance une contre-mesure si un processus gagne les droits du super utilisateur (root) sans être passé par l'un des appels système prévus pour cela. Ceci détecte aussi de nombreuses autres attaques "local-to-root", incluant do_mmap, do_munmap, do_mremap... lesquelles n'ont été connues que par la suite. ORCHIDS peut donc détecter certaines "zéro-day attacks".



L'attaque mod_ssl de 2003 permet d'obtenir une ligne de commande à distance ("remote exploit"), via l'insertion d'un shellcode, utilisant un débordement de tampon en mémoire (ci-dessus). On peut ensuite rejouer une attaque local-to-root comme ptrace ou do_brk pour obtenir les droits du super utilisateur.



La base de signatures d'ORCHIDS.



ORCHIDS fait échouer une instance de l'attaque ptrace. L'intrus est expulsé, et son compte est fermé.