Rapport du projet SELinux

Prof Gérald Litzistorf – hepia – octobre 2014 – www.tdeig.ch

§1 Chapitre scientifique

§1.1 Modèles de sécurité des systèmes d'information

La majorité des systèmes d'information publics et privés (postes de travail, serveurs DNS – web – base de données, proxy, firewall, …) reposent sur un composant central qui est le **système d'exploitation** (Windows, Linux, …Android). Ce type de logiciels possède une architecture logicielle très ancienne basée sur un noyau (NT / Linux kernel) qui offre la notion d'entité d'exécution (thread & processus) indépendante à ses utilisateurs.

Afin d'assurer un **cloisonnement** entre ces divers processus (applications, services DNS – web, …), chacun reçoit un jeton d'accès hérité lors de son lancement ; ainsi sur un poste Windows divers services (DHCP, DNS, …) sont démarrés lors du boot avec le compte Système avant qu'un utilisateur puisse s'authentifier avec un compte utilisateur.

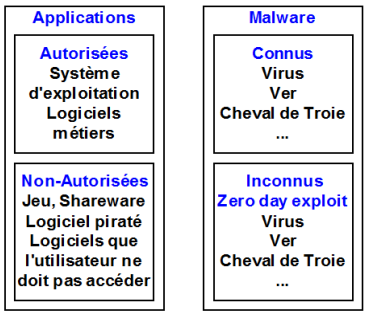
Le modèle de sécurité de ces systèmes d'exploitation repose sur un *Reference Monitor* et un accès discrétionnaire **DAC** *(Discretionary Access Control)* : chaque ressource (fichier, …) possède une liste blanche des utilisateurs (groupes) autorisés à lire – écrire – exécuter ce fichier. L'accès à la ressource est obtenu si le processus hérite d'un jeton approprié qui indique l'identifiant de l'utilisateur (ou groupe).

Etant donné que ces systèmes basent leur sécurité sur la notion de compte utilisateur, la méthodologie d'attaque consiste souvent à exploiter une **faille du système** afin d'obtenir un accès avec les droits maximum. Dans le cas du ver Blaster, le code malveillant s'attaquait à un système Windows XP SP1, présentant une faille de type *buffer overflow in Microsoft's Remote Procedure Call (RPC) implementation*, afin d'obtenir un *remote shell* avec les droits Système via le port TCP 4444. Outre la mise à disposition d'un correctif, la réponse sécuritaire a été d'activer un *personnal firewall* comme outil de défense périmétrique dans Windows XP SP2.

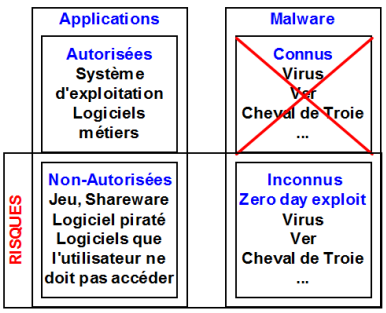
L'exemple ci-dessus illustre le principe de **défense en profondeur** : si le premier rempart *(personnal firewall)* tombe ; un autre dispositif (le correctif dans l'exemple) protège le système de cette intrusion.

Pour protéger au mieux un système, il convient d'analyser les risques potentiels ainsi que les besoins opérationnels. Les figures ci-dessous illustrent la problématique du poste de travail en entreprise (source SecureWave)

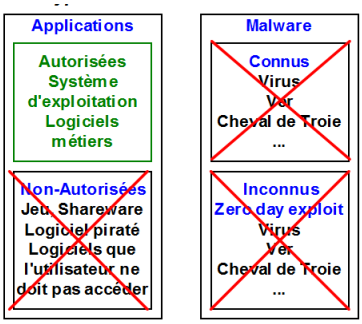
Principaux risques



Protection de type liste noire (liste d'exclusion)



Protection de type liste blanche (liste d'inclusion)



Parmi les codes (virus, vers, …) malveillants *(malware)*, distinguons les anciens connus de votre antivirus et les autres (celui qui a été créé la nuit passée) potentiellement dangereux car inconnus ***(zero day exploit)*** des listes noires.

Seule une politique de sécurité basée sur un modèle de **liste blanche** permet d'obtenir le résultat escompté à savoir que l'utilisateur ne peut exécuter que les applications autorisées. On parle aussi de modèle comportementale.

§1.2 Contexte et cadre général du projet

SELinux constitue aujourd'hui le nec plus ultra pour sécuriser efficacement des systèmes Linux. Selon les auteurs du livre *SELinux by Example* : *SELinux represents the culmination of nearly 40 years of operating system security research*.

SELinux implémente divers modèles de sécurité (MAC, RBAC, Bell-LaPadulla) qui doivent être maîtrisés pour améliorer le niveau de sécurité des serveurs actuels. Trop de personnes estiment que SELinux est trop complexe par manque de connaissance. Désactiver SELinux aujourd'hui sur un serveur revient à ne pas être capable de régler la hauteur de son appuie-tête en voiture.

Les premiers travaux d'étudiants réalisés avant ce projet montrent un indéniable gain sécuritaire et des difficultés à en maîtriser tous les aspects. Chaque paquetage d'une distribution Linux est livré avec des règles SELinux qui peuvent parfois poser problème.

L'essentiel du travail va donc consister à définir des **scénarios** précis pour proposer la bonne **méthodologie** utilisant les bons outils parmi les très nombreux proposés.

Parmi ces scénarios, nous comptons étudier comment SElinux peut améliorer le cloisonnement entre machines virtuelles. Nous proposons de mettre en place une **défense en profondeur** très robuste pour des architectures virtualisées basées sur Linux-KVM critiques au niveau de la sécurité.

Face à une technologie SELinux complexe et éprouvée, nous estimons que son potentiel de sécurisation doit être accessible à notre économie ; ce processus (projet) exige les ressources (**temps**) nécessaires pour en comprendre les principaux éléments et offrir des formations spécifiques.

Cette forme **d'innovation** convient parfaitement à une HES.

§1.3 Résultats obtenus avec description des livrables

Ce projet financé par le RCSO-TIC est de type exploratoire ; il a donc pour objectif l'acquisition de compétences dans le contexte décrit au §1.2

Tous les documents mentionnés se trouvent dans http://www.tdeig.ch/SELinux/
La liste ci-dessous est classée par ordre de complexité croissante

a) Travail de Bachelor Security Enhanced for Linux de Khaled Basbous
Premiers travaux effectués au labo
Le domaine est complexe et justifie un financement
Les divers mécanismes offerts par SELinux peuvent augmenter le niveau de sécurité d'un système sur le principe de la défense en profondeur
http://www.tdeig.ch/linux/Basbous_RTB.pdf

b) Résumé des fonctionnalités et des outils
Une fois les concepts théoriques acquis, les outils permettent des mises en œuvre spécifiques
La multitude des outils surprend au début
http://www.tdeig.ch/SELinux/b_Fonctionality_admin_tools.pdf

c) Contenu et organisation de la formation Red Hat
Offre de formation d'un leader du monde Open Source ; l'offre est très riche
http://www.tdeig.ch/SELinux/c_Formation_RedHat.pdf

d) Cours Bachelor 3ème hepia
Premier résultat destiné aux étudiants ITI
Quels sont les principaux mécanismes ?
A quoi servent-ils ?
Cohabitation de SELinux avec le modèle de sécurité de base de Linux
http://www.tdeig.ch/SELinux/d_Slides.pdf

e) Labo Bachelor 3ème hepia
Complément pratique au cours précédent
Plusieurs itérations ont été nécessaires pour atteindre la perfection ?
http://www.tdeig.ch/SELinux/e_Labo.pdf

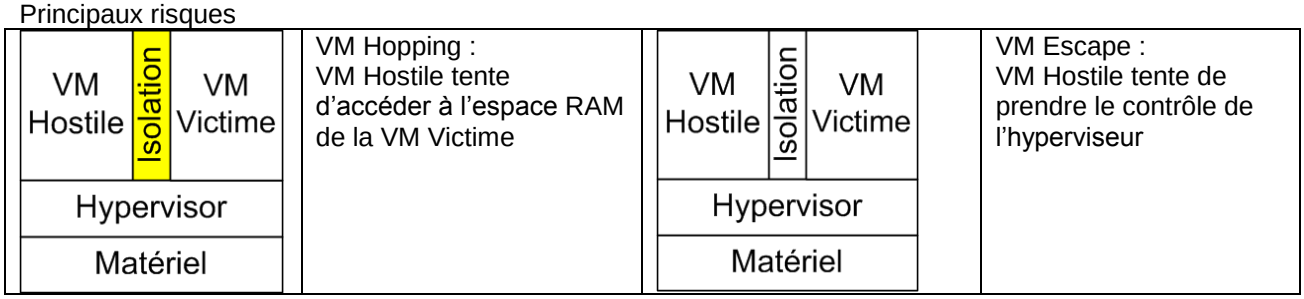
f) Travail de Bachelor SELinux de Kevin Carli – écriture d'un policy module
SELinux est le fruit de quelques spécialistes (Walsh, …)
A chaque version de Fedora, il protège encore mieux le système bien qu'il ne puisse pas offrir une sécurité à 100%
Il se concentre donc sur les risques jugés majeurs tels que la sécurisation d'un serveur (DNS, web, …) accessible depuis internet.
Ainsi les packages que l'ingénieur choisit puis configure contiennent généralement les règles SELinux.
L'objectif de ce travail de Bachelor est d'écrire un module de sécurité comme devrait le faire un éditeur de logiciel souhaitant activer les mécanismes SELinux
http://www.tdeig.ch/linux/Carli_RTB.pdf

g) Cheminement d'investigation pour compiler et installer un service selon les bonnes pratiques
Ce document démontre que le procédé de sécurisation d'un service doit être réalisé avec minutie.
Le cloisonnement du service doit être testé avec des scénarios de « pentesting » pour s'assurer que la configuration réalisée est bien faite.
Ce document présente la méthodologie utilisée qui a conduit à définir les bonnes pratiques.
http://www.tdeig.ch/SELinux/g_Best_Practice_Secure_Software.pdf

h) Labo zero-day (adaptation pour Fedora 18) pour Master
Ce document est certainement le plus intéressant puisqu'il démontre que la mise en œuvre correcte de SELinux permet de contrer une attaque de type zero-day
Nous nous basons sur une attaque réelle pour montrer la puissance de SELinux tout en rappelant que seul un modèle inclusif (white-list) peut faire face à ce type fréquent d'attaque.
http://www.tdeig.ch/SELinux/h_Lab_ZeroDay.pdf

i) Sandboxing KVM/LXC
Les architectures virtualisées avec ESXi (VMware) ou KVM (Linux) ont bonne réputation dans le cloisonnement des machines virtuelles

Principaux risques



Dans un modèle de défense en profondeur, quels sont les mécanismes SELinux garantissant ce cloisonnement
http://www.tdeig.ch/SELinux/i_Sandboxing.pdf

j) Isolation des machines virtuelles avec sVirt
Même problématique que i)
http://www.tdeig.ch/SELinux/j_VMs_Isolation.pdf

k) Evolution et changements entre Fedora 16 et Fedora 19
Chaque version de Fedora devrait être mieux protégée par SELinux
Quelles sont les principaux changements ?
http://www.tdeig.ch/SELinux/k_F16vsF19.pdf

l) Analyse sécuritaire OpenStack
En complément au TM de Benoît Chalut http://www.tdeig.ch/linux/Chalut_RTM.pdf, nous avons réalisé une analyse des risques du monde Cloud. Cette étude a guidé et focalisé nos efforts de sécurisation sur les nœuds hyperviseurs d'OpenStack.
La validation du cloisonnement des VMs a été réalisée selon les bonnes pratiques défini en g).
http://www.tdeig.ch/SELinux/l_Analyse_securitaire_Openstack.pdf

m) Liens utiles
http://www.tdeig.ch/linux/liens_KVM.pdf

§1.4 Volet économique & valorisation

Des personnes de cinq entreprises de Suisse romande ont été contactées.
Le résultat a été très décevant au point que l'assistant qui pensait initialement effectuer son TM dans le domaine a préféré choisir un domaine de l'informatique plus porteur en termes d'employabilité en Suisse romande.

Proches du profil ingénieur des systèmes d'information, je n'ai pas assez investigué parmi les entreprises qui développent du logiciel compatible Linux et qui doivent garantir à leurs clients le respect des bonnes pratiques sécuritaires (dont Linux fait partie).

§1.5 Valorisation au sein de la HESSO

Une journée de formation destinée au personnel HESSO a été organisée le 4 juin 2014 à hepia.

- 4 personnes de HEIG-VD ont participé (Prof. Junod – Pasini, Assistant Rinaldini - Wehrli)
- Prof Buntsch (EIA-FR) et prof Ertz (HEIG-VD) ont reçu les supports pédagogiques car ils ne pouvaient pas participer

§1.6 Volet pédagogique

Parmi les motifs évoqués dans la demande de financement figurait le constat que la technologie SELinux n'était pas enseignée dans notre HESSO en 2011-2012.

Nos étudiants Bachelor ont donc été les premiers à utiliser et tester ce matériel pédagogique développé dans le cadre de ce projet.

Le §1.3 montre une forte interaction entre ce financement et les activités du labo

- Deux travaux de Bachelor → voir §1.3a) et §1.3f)
- Des supports d'enseignement (niveaux Bachelor & Master) → voir §1.3d), §1.3e) et §1.3h)
- Un complément d'étude à TM → voir §1.3l)
- Des compléments d'étude à la virtualisation → voir §1.3i) et §1.3j)

§1.7 Conclusion

SELinux constitue un ensemble de dispositifs sécuritaires puissants et éprouvés adaptés aux besoins de l'économie.

Basés sur un modèle inclusif (white-list), ils permettent de mettre en œuvre une excellente défense en profondeur sur des serveurs jugés critiques au niveau sécuritaire.

Le lecteur devrait être persuadé qu'il est plus efficace d'investir dans des modèles inclusifs que dans les traditionnels modèles exclusifs comme un antivirus.

L'attaque de type zeroday, dont seul le hacher connait le mode opérationnel, ne peut être contrée avec les modèles exclusifs qui ne connaissent que les attaques anciennes.

En 2012 en typant SELinux dans google, la première proposition était disabled ; 2 ans plus tard elle arrive en 3ème position derrière centos et status.

SELinux apporte donc un réel gain sécuritaire au prix d'une certaine complexité.
Puissent les livrables produits dans ce projet aider certains à ne pas désactiver SELinux !
Voir des illustrations dans §1.3 e) Blocages

§2 Chapitre administratif

§2.1 Ressources engagées

Khaled Basbous, qui a effectué son travail de Bachelor au laboratoire (voir §1.3 a), a été engagé comme assistant du 1 sept 2012 au 31 août 2014 sur ce projet en plus d'activité d'encadrement pédagogique.

§2.2 Calendrier

Prévu initialement sur une période de 12 mois à partir de sept 2012, ce projet a été étalé sur 2 ans pendant lesquelles Khaled Basbous a suivi le MSE.