h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Printemps 2012
Session de bachelor

SECURITE DES SYSTEMES D'INFORMATION

SELINUX

Descriptif :

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 réalisés par les étudiants Gattuso - Roschi 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 ; voir l'illustration par Fedora avec le serveur Apache
→ http://doc.fedora-fr.org/wiki/Installation_et_configuration_d%27Apache#SELinux_et_apache

Travail demandé :

1. Introduction
   Parcourir le livre SELinux by Example http://flylib.com/books/en/2.803.1.1/1/ pour identifier l'éventail des possibilités offertes ainsi que les outils proposés
   Etude du rapport http://www.tdeig.ch/Soir3/Rapport_Final/Roschi_Gattuso_SELinux.pdf
   Lien utile : https://fedoraproject.org/wiki/SELinux
   Estimation = 2 semaine

2. Comprendre le fonctionnement de SELinux avec les règles par défaut de Fedora 16
   Identifier les outils utiles
   Etudier quelques cas simples de règles fournies dans des packages
   Estimation = 2 semaines

3. Expliquer l'architecture de SELinux
   Utiliser la présentation de *School of Computer Science and Engineering, Seoul National University*
   - http://ssrnet.snu.ac.kr/course/sec2007-1/note/SELinux-2007.ppt
   - http://www.tdeig.ch/TB_2012/SELinux/SELinux-2007.ppt copie locale

   Voir les slides 29-34 qui illustrent l'évolution de l'architecture SELinux depuis le projet Flask (slide 30) jusqu'à son implémentation.
   Estimation = 2 semaines

4. Configurer une sécurité basée sur le modèle Bell-LaPadulla : *No information flow from 'high' security levels down to 'low' security level (confidentiality)*
   Estimation = 1 semaine

5. Thème à choix si le temps le permet

   Sous réserve de modification en cours du travail de Bachelor

Candidat :
M. BASBOUS KHALED
Filière d'études : --
Domaine de formation --

Professeur(s) responsable(s) :
Litzistorf Gérald

En collaboration avec : Nom de l'entreprise
Travail de bachelor soumis à une convention de stage en entreprise : non
Travail de bachelor soumis à un contrat de confidentialité : non

Timbre de la direction