Atelier sécurité - première partie

Introduction générale à la sécurité

Victor Stinner

Club des utilisateurs de logiciels libres de l'UTBM

Lolut Automne 2005

Sommaire

Sécurité = disponibilité

- « La sécurité informatique a pour but de garder un ordinateur opérationnel dans n'importe quelle condition »
- Tolérance aux pannes matérielles
- Tolérance aux pannes logicielles

Sécurité = confidentialité

- « La sécurité informatique a pour but d'assurer que les ressources ne sont accessibles qu'aux personnes autorisées »
- Gestion fine des droits
- Système d'authentification robuste
- Peut utiliser le chiffrement des données et la signature des documents

Sécurité = intégrité

- « La sécurité informatique a pour but d'assurer que les données ne sont pas modifées, altérées ou détruites »
- Intégrité lors du stockage et du transfert des données

La sécurité est la combinaison des trois

- Disponibilité
- Confidentialité
- Intégrité

Sommaire

Enjeux de la sécurité

- Le ver Code Red a causé des dégats de l'ordre de milliards de dollar US (!).
- Vol de données (ex : numéros de carte de crédit, espionnage industriel).
- Des bris de sécurité peuvent causer du tort à la vie privée et à la confidentialité.

Quelques risques liés à la sécurité

- Corruption et perte des données (ver, virus)
- Intrusion dans le système (trojan, exploit, rootkit)
- Envoi d'informations à notre insu (spyware)

Sommaire

Principe du maillon faible

- La sécurité d'un système est celle de l'élément le plus faible.
- Il faut connaitre tous les éléments du système, ne rien négliger.
- Rien ne sert d'installer une porte blindée sur un mur en carton.

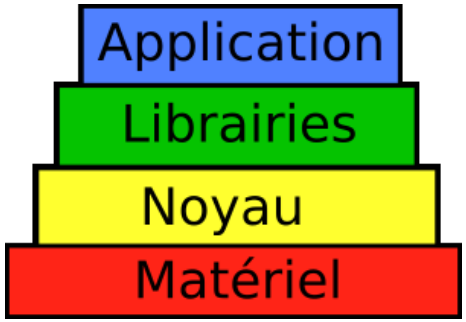
Exemple : Authentification sur un ordinateur (local)

- Choix des mots de passe.
- Est-ce que le bootloader (Lilo/Grub) est sécurisé ?
- Est-ce que le BIOS est sécurisé ?
- Est-ce que l'ordinateur est physiquement sécurisé ?
  (fermé par un cadenas et attaché au bureau)

Exemple : Faille dans Linux

Architecture d'un ordinateur

- Applications : Firefox, Gimp, Gvim, Xchat, etc.
- Bibliothèques : libc, zlib, GTK, X11, etc.
- Noyau : Linux, OpenBSD, Hurd, etc.
- Matériel : Processeur, mémoire, carte vidéo, chipset, etc.



Exemple : Faille dans Linux

Faille chown

- Linux est développé par des humains, et du coup est faillible. Des failles sont régulièrement découvertes dans le noyau.
- Exemple : faille permettant de changer le propriétaire (groupe) d'un fichier dans les version inférieures à 2.4.28 et 2.6.8. Voir l'exploit : www.0xdeadbeef.info/exploits/raptor_chown.c

Exemple : Faille dans Linux

Extrait de l'exploit chown

chown(argv[1], -1, getgid()) ;

- argv[1] : Nom du fichier
- -1 : Propriétaire du fichier, -1 signifie "pas de changement"
- getgid() : Groupe du fichier, utilise le groupe de l'utilisateur ayant lancé le programme.