Faculté des Sciences de Limoges — 2002–2003
DESS Sécurité de l'Information
Cryptographie

Travaux pratiques, séance 4

Partition chiffrée

Linux offre plusieurs possibilités pour chiffrer des fichiers ou des partitions. L'une d'entre elles consiste à créer une partition à l'intérieur d'un fichier créé pour l'occasion.

Le noyau Linux trouvé sur le serveur officiel `www.kernel.org` et dont Linus Torwalds dirige le développement est dépouillé de tout algorithme cryptographique, en raison des lois américaines sur la cryptographie. Un patch dit "international", autrefois disponible sur un serveur séparé au Danemark est maintenant maintenu par Herbert Valerio Riedel et disponible sur sa page (`www.kernel.org/pub/linux/kernel/people/hvr`).

1. — Extraire les sources du noyau et recopier la configuration de votre noyau actuel :

```
$ tar -xjf linux-2.4.19.tar.bz2
$ cd linux-2.4.19
$ cp /usr/src/.config .              % récupérer la config actuelle
```

2. — (Optionnel.) Configurer votre futur noyau avec la commande `make menuconfig`. Vous pouvez alléger votre noyau en désactivant (touche `n`) les options indiquées ci-dessous. Pour activer une option en intégrant le code directement dans le noyau, taper `y`. Pour intégrer le code dans un module, taper `m`.

- General Setup ⟶ PCMCIA/CardBus support : No
- Memory Technology Support : No.
- Multi-device support/RAID & LVM : No.
- Networking Options/Packet Socket : Yes (au lieu de Module).
- Telephony Support : No.
- SCSI Support : No.
- IEEE 1394 (FireWire) Support : No.
- Amateur Radio Support : No.
- IrDA Support : No.
- ISDN Support : No.
- Old CD-ROM drivers Support : No.
- Multimedia support ⟶ Video for Linux : No.
- BlueTooth support : No. Quitter l'utilitaire de configuration et répondre `Yes` à `Save?`.

3. — Patcher les sources du noyau :

```
$ patch -p1 < path_to_file/loop-jari-2.4.18.0.patch
$ bzcat path_to_file/patch-int-2.4.19.2.bz2 | patch -p1
```

Refaire `make menuconfig` pour configurer les nouvelles options.

- Block Devices/Loopback Device Support : "Yes" au lieu de "Module".
- Cryptographic Options/
  — Cryptographic API Support : "Yes".
  — Cryptographic Ciphers : "yes". Configurer aussi en "Module" tous les algorithmes proposés.
  — Message Digest : "yes". Configurer aussi en "Module" tous les algorithmes proposés.
  — Crypto Devices : "yes"
  — Loop Crypto support : "yes"
  — IPSEC Tunneling : "Module" (?)

4. — Compiler votre nouveau noyau (vous avez le temps d'aller prendre l'air).

```
$ make clean
$ make dep
$ make bzImage
$ make modules
$ make modules_install
$ cp -p arch/i386/boot/bzImage /boot/vmlinuz-2.4.19i
```

5. — Installer le nouveau noyau : éditer `/etc/lilo.conf` et y rajouter l'option suivante :

```
image=/boot/vmlinuz-2.4.19i
        label=linux-crypto
        root=/dev/hda5
        read-only
```

Lancer la commande `lilo` pour mettre à jour le MBR.

6. — Rebooter `shutdown -r now` avec le nouveau noyau et croiser les doigts...

7. — Récupérer une archive de Util-Linux, patcher et recompiler les commandes `mount`, `umount` et `losetup`.

```
$ tar -xjf util-linux-2.11v.tar.bz2
$ cd util-linux-2.11v
$ bzcat path_to_file/util-linux-2.11r.patch.bz2 | patch -p1
$ ./configure
$ make
$ mv /bin/mount /bin/mount.orig
$ mv /bin/umount /bin/umount.orig
$ mv /sbin/losetup /sbin/losetup.orig
$ cd mount
$ cp -p mount /bin
$ cp -p umount /bin
$ cp -p losetup /sbin
$ chmod u+s /bin/mount /bin/umount
```

Attention : surtout ne **pas** faire `make install` !

8. — Créer la nouvelle partition : en tant qu'utilisateur standard, créer le fichier destiné à recevoir la partition (ici, fichier `.secretloop` de 100 k-octets).

```
$ dd if=/dev/zero of=.secretloop bs=1k count=100
```

En tant que root, attacher ce fichier à `/dev/loop0`, en utilisant Rijndael-128 (par exemple).

```
$ losetup -e aes /dev/loop0 .secretloop
Keysize: 128
Password: <clé de chiffrement>
$ mkfs -t ext2 /dev/loop0
```

9. — Monter, utiliser, et démonter la partition chiffrée.

```
$ mount -t ext2 /dev/loop0 /mnt/disk
$ <utiliser la partition...>
$ umount -d /dev/loop0
```

10. — Créer le répertoire `~/secret` et mettre dans `/etc/fstab` la ligne suivante.

```
/home/untel/.secretloop /home/untel/secret ext2 user,noauto,loop,encryption=aes 0 0
```

En tant qu'utilisateur quelconque, vous pouvez monter la partition par la commande `mount secret` et en donnant la clé. Démonter par `umount secret`.