https://clx.asso.fr/spip/?Chiffrer-les-partitions-de-swap

Mandrake 8.2

Chiffrer les partitions de swap

- Documentations - Installation / Administration de base de Linux -

Date de mise en ligne : samedi 13 avril 2002

Ce patch nous viens de la ML Open-Crypto de Michel Bouissou.

J'ai testé pour vous ce correctif de la Mandrake 8.2 et ça marche. (C'est un bug spécifique à la Mandrake 8.2)

La version d'origine se trouve ici.

N.B. :
– Ce patch de rc.sysinit a été réalisé UNIQUEMENT pour une Mandrake 8.2 et n'est probablement PAS compatible avec une autre distribution.
– Dans tous les cas de figure, ce patch nécessite la présence de loop-aes sur le systÚme (qui est inclus avec le noyau standard sur la Mandrake 8.2).
– L'utilisation de ce patch avec une autre distribution est susceptible de créer des problÚmes. Vous avez été prévenu ;-)
– Dans tous les cas de figure, l'utilisation de ce patch est entiÚrement à vos risques et périls, et je n'assume aucune responsabilité, ni ne fournis aucune espÚce de garantie, etc.
– Ce patch s'appliquant au script rc.sysinit sous licence GPL, est lui-même également sous licence GPL.

"La Mandrake 8.2, qui inclut le système loop-aes, permet supposément de chiffrer les partitions de swap de manière très facile.

Malheureusement, un bug dans /etc/rc.d/rc.sysinit fait que cela ne fonctionne pas. J'ai trouvé le bug, et écrit un patch correctif que je joins en attachement de ce message."

Installation du patch (en console root) :

Ce patch ce nomme doc19.gz sur le site du CLX. Renommez le en rc.sysinit.patch.gz ou adaptez les commandes ci-dessous.

Copier rc.sysinit.patch.gz *(ou doc19.gz)* dans /etc/rc.d, puis :

```
cd /etc/rc.d
 gunzip rc.sysinit.patch.gz (ou doc19.gz)
 patch < rc.sysinit.patch
```

Mise en oeuvre d'un swap chiffré :

Il suffit d'éditer /etc/fstab, et de modifier la ligne définissant le (ou les) swap(s) comme suit (exemple) :

```
/dev/hda4 swap swap defaults 0 0
```

qui devient

```
/dev/hda4 swap swap encrypted 0 0
```

...puis de rebooter le système.

Le swap sera alors automatiquement chiffré par AES128 en utilisant une clé de session aléatoire différente à chaque démarrage.

Une fois la machine redémarrée, il est facile de contrôler que le swap est désormais chiffré, par exemple :

```
[root@totor etc]# swapon -s
 Filename                        Type            Size    Used    Priority
 /dev/loop/0                     partition       128512  0       0
 /dev/loop/1                     partition       128512  0       0
```

```
[root@totor etc]# losetup /dev/loop/0
 /dev/loop/0 : [0007]:447 (/dev/hda4) décalage 0, AES128 cryptage
```

```
[root@totor etc]# losetup /dev/loop/1
 /dev/loop/1 : [0007]:747 (/dev/sda3) décalage 0, AES128 cryptage
```

https://clx.asso.fr/spip/local/cache-vignettes/L64xH64/gz-96c51.svg

rc.sysinit.patch.gz

Patch correctif pour chiffrer
la swap d'une Mandrake 8.2.
A renommer en rc.sysinit.patch.gz
aprÚs le téléchargement.

Post-scriptum :

La clé est générée par mcookie (man mcookie).

Une clé de session aléatoire est générée par mcookie à chaque boot, et est différente pour chaque swap (si l'on utilise plusieurs swaps) ;

Le programme mcookie utilise pour s'initialiser les éléments suivants :
– Un mélange de différents paramÚtres pseudo-aléatoires du systÚme à l'entropie probablement faible au démarrage : Timer, NÂ° de pid...
– 64 octets provenants de /dev/urandom (sur une Mandrake 8.2), ou 16 octets de /dev/random (sur d'autres distribs). L'entropie de /dev/random est
probablement bonne, tandis que celle de /dev/urandom peut éventuellement laisser à désirer peu de temps aprÚs le démarrage du systÚme.
– 40 K octets tirés du swap chiffré tel qu'il était au démarrage de la machine, avant que celui-ci ne soit immédiatement écrasé par de nouvelles données pseudo-aléatoires (par chiffrement de zéros avec la nouvelle clé de session). Le contenu du swap chiffré au démarrage de la machine est trÚs hautement aléatoire, et ceci me semble donc constituer une excellente source
d'entropie d'appoint.

L'utilitaire mcookie faisant un mélange de tous ces éléments avant d'en ressortir un hash md5, il me semble que la clé de session obtenue en sortie offre toutes les garanties d'entropie nécessaires à une utilisation en toute sécurité.