Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Encriptant particions (9464 lectures)

Per **Albert Sellarès**, ***whats*** (http://www.wekk.net)

Creado el 17/07/2004 13:25 modificado el 17/07/2004 13:37

Els sistemes de xifratge són cada vegada més importants, el fet d'haver de protegir les nostres dades, fa que hàgim de recórrer a mètodes de xifratge, per tal que en cas de caure en males mans, no pugui ser utilitzada.

Jo ja portava un temps amb la intenció de mirar-me com fer-ho, i ara aprofitant que he acavat els exàmens, m'he pres un descans i he començat a buscar com poder estar tranquil deixant les meves dades a casa quan jo no hi sóc :P

Aquí explicaré com xifrar una una partició per tal de que si mai us robessin el disc dur o algú aconsegus accès físic a la vostre màquina, els fos "impossible" arribar a accedir al vostre contingut.

Aquest article també el podeu trobar a Catux[1]

ALGUNS CONCEPTES:

Una "device-mapper" és una nova infraestructura(dm-crypt) que ens permet crear capes virtuals sobre dispositius de blocks d'una forma genèrica, gràcies a ella, podem arribar a fer moltes coses amb els nostres dispositius, un exemple d'elles seria tractar dos particions com si focin una sola, o la que tractarem que és afegir una capa de xifratge a elles.

En concret nosaltres crearem un nou dispositiu de blocks a /dev en el que tot el que hi escrivim s'encriptarà i tot el que llegim es xifrarà automàticament.

Montarem el nostre sistema de fitxers de forma usual, però si no entrem la nostre frase de pas, no podrem accedir a les nostres dades.

En principi fer tot això amb el dm-crypt, és força millor que el sistema que utilitza el cryptoloop(tal com diu el propi mantenidor) per forces raons:

-És suportat el fet de muntar arxius
-No pateix els bugs del loop.c que al no tenir mantenidor, se'n troben forces
-dm-crypt no depen de cap aplicació especial (util-linux)
-dm-crypt usa mempool, cosa q el fa molt més estable i segur
En definitiva, una "device-mapper" forma part de la nova tecnologia del kernel.

Aquí podeu trobar totes les deficiències del cryptoloop (http://lwn.net/Articles/67216/[2])

SUPORT DEL KERNEL:

Aquestes noves característiques es van afegir a la versió 2.6.4 de linux, per tant necessiteu aquesta o una versió superior per a poder-les usar.

Les opcions que hem d'activar són:

Primer haurem d'activar que ens mostri les opcions en desenvolupament:

Code maturity level options ---> Prompt for development and/or incomplete code/drivers

Després activar el device mapper i el support per encriptar-lo:
Device Drivers ---> Multi-device support (RAID and LVM) --->
[*] Multiple devices driver support (RAID and LVM)
Device mapper support
Crypt target support

Ara només ens faltarà activar els algoritmes d'escriptació:

Cryptographic options --->

Aquí els podeu activar tots, va molt a gustos. Jo us recomano el nou "AES cipher algorithms", ja que es comporta molt bé per x86 treballant força ràpid i donant un fort xifratge.

Tot i així, potser us interessen uns benchmarks per acabar-vos de decidir :)

http://www.saout.de/tikiwiki/tiki-index.php?page=UserPageChonhulio[3]

EINES D'USUARI:

Dons com sempre agraïm tenir una vida "tant fàcil" els que usem debian i podem instal·lar els dos paquets necessaris via apt-get :)

Instal·lem les aplicacions d'usuari per al device-mapper:

apt-get install dmsetup

I una aplicació per tal que la nostra frase de pas faci millor la seva feina ;)

apt-get install hashalot

Per últim podem descarregar-nos un script que ens permetrà fer la feina de crear els nostres dispositius d'una manera més fàcil: http://www.saout.de/misc/dm-crypt/cryptsetup.sh[4]

CREACIÓ DESL DISPOSITIU DM-CRYPT

Primer de tot haurem de triar una partició, suposem /dev/hda5 (ha d'estar desmontada!)

executem:

root@wekk.net:~# sh cryptsetup.sh -c aes -h ripemd160 -y -b `blockdev --getsize /dev/hda5` create cryptdev1 /dev/hda5
Enter passphrase:

El que fa és crear-nos un dispositiu anomenat cryptdev1 (/dev/mapper/cryptdev1) utilitzant l'algoritme "aes" (podeu consultar els que suporta el vostre kernel amb cat /proc/crypto que seran els que heu afegit vosaltres avans :P), la frase de pass serà entrada usant el tipus de hash "ripemd160" (no tinc cap preferència en quin usar...)

Un cop fet això ja disposareu del vostre dispositiu xifrat!, el formatejarem ....

root@wekk.net:~# mkreiserfs /dev/mapper/cryptdev1

i el montem:

root@wekk.net:~# mount /dev/mapper/cryptdev1 /mnt/crypto

i ja disposem de la nostre partició encriptada!

A partir d'ara cada vegada que re iniciem la màquina haurem de crear el dispositiu. Si la caguem al posar la paraula de pass, al intentar montar el sistema rebrem un bonic missatge:

```
root@wekk.net:~# sh cryptsetup.sh -c aes -h ripemd160 -y -b `blockdev --getsize /dev/hda5` create cryptdev1
/dev/hda5
Enter passphrase: (la posem malament)

root@wekk.net:~# mount /dev/mapper/cryptdev1 /mnt/crypto
mount: you must specify the filesystem type
```

Ja tenim les dades protegides de tot perill!

eliminem el dispositiu, i tornem a posar la frase de pas..

```
root@wekk.net:~# sh cryptsetup.sh remove cryptdev1
root@wekk.net:~# sh cryptsetup.sh -c aes -h ripemd160 -y -b `blockdev --getsize /dev/hda5` create cryptdev1
/dev/hda5
Enter passphrase:

root@wekk.net:~# mount /dev/mapper/cryptdev1 /mnt/crypto
```

CONFIGURACIÓ A L'ARRENCADA:

Si us interessa fer que cada vegada que us arrenca el pc es monti la partició, podeu fer-ho així:

```
#!/bin/bash

case $1 in
start)
echo -n "Iniciant dm-crypt, entra la frase de pas:" /usr/local/sbin/cryptsetup.sh -c aes -h ripemd160 -b `blockdev
--getsize /dev/hda5` create cryptdev1 /dev/hda5
/bin/mount /dev/mapper/cryptdev1 /mnt/crypt/
echo "Fet!"
;;

stop)
echo -n "Eliminant dm-crypt... "
/bin/umount /mnt/crypt/
/usr/local/sbin/cryptsetup.sh remove cryptdev1
echo "Fet!"
;;
*)

echo "$0 start|stop"
esac
```

Aquest script es podria millorar facilment fent q si amb 10 segons no s'ha escrit el pass que arrenqui de manera normal, però això us ho deixo per vosaltres :)

```
root@wekk.net:~# cp cryptdev /etc/init.d/

root@wekk.net:~# chmod 755 /etc/init.d/cryptdev

root@wekk.net:~# update-rc.d cryptdev defaults
Adding system startup for /etc/init.d/cryptdev ...
/etc/rc0.d/K20cryptdev -> ../init.d/cryptdev
/etc/rc1.d/K20cryptdev -> ../init.d/cryptdev
/etc/rc6.d/K20cryptdev -> ../init.d/cryptdev
/etc/rc2.d/S20cryptdev -> ../init.d/cryptdev
```

/etc/rc3.d/S20cryptdev -> ../init.d/cryptdev
/etc/rc4.d/S20cryptdev -> ../init.d/cryptdev
/etc/rc5.d/S20cryptdev -> ../init.d/cryptdev

I a partir d'ara cada vegada que arrenqueu, us demanarà la frase de pas per a poder montar després la partició.

El que es podria fer per estalviar-se el password, és passar-li l'opcio "-d arxiu" al cryptsetup.sh, per tal d'usar la clau dins "d'arxiu" per a encriptar la partició amb l'algoritme triat. Aquesta clau podria estar a un dispositiu d'aquests usb que estan tant de moda, i així aconseguirem que si no hi ha el usb posat, el pc no arrenqui o simplement no es monti la partició xifrada.

Una altre cosa molt interessant de fer, és que la swap també sigui xifrada. D'aquesta manera aconseguim estar segurs que a la part del disc que s'ha usat com a memòria, tampoc hi han dades sensibles.

Per fer-ho haurem de treure del nostre /etc/fstab la línia que activa la swap
/dev/hda6 none swap sw 0 0

i afegirem aquest altre script amb el nom de cryptswap

```
#!/bin/bash

case $1 in
start)
#Iniciant swap-crypt
/usr/local/sbin/cryptsetup.sh -c aes -h ripemd160 -d /dev/random -b `blockdev --getsize /dev/hda6` create cryptswap
/dev/hda6
/sbin/mkswap /dev/mapper/cryptswap
/sbin/swapon /dev/mapper/cryptswap
;;

stop)
#Iniciant swap-crypt
/sbin/swapoff /dev/mapper/cryptswap
/usr/local/sbin/cryptsetup.sh -c aes -h ripemd160 -d /dev/random -b `blockdev --getsize /dev/hda6` create cryptswap
/dev/hda6

;;
*)

echo "$0 start|stop"
esac
```

```
root@wekk.net:~# cp cryptswap /etc/init.d/

root@wekk.net:~# chmod 755 /etc/init.d/cryptswap

root@wekk.net:~# update-rc.d cryptswap defaults
Adding system startup for /etc/init.d/cryptswap ...
/etc/rc0.d/K20cryptswap -> ../init.d/cryptswap
/etc/rc1.d/K20cryptswap -> ../init.d/cryptswap
/etc/rc6.d/K20cryptswap -> ../init.d/cryptswap
/etc/rc2.d/S20cryptswap -> ../init.d/cryptswap
/etc/rc3.d/S20cryptswap -> ../init.d/cryptswap
/etc/rc4.d/S20cryptswap -> ../init.d/cryptswap
/etc/rc5.d/S20cryptswap -> ../init.d/cryptswap
```

Dons ja sabeu, a partir d'ara ja podreu dormir tranquils!!

Lista de enlaces de este artículo:

1. http://www.catux.org
2. http://lwn.net/Articles/67216/
3. http://www.saout.de/tikiwiki/tiki-index.php?page=UserPageChonhulio
4. http://www.saout.de/misc/dm-crypt/cryptsetup.sh

E-mail del autor: whats _ARROBA_ wekk.net