Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Encriptando particiones o todo tu sistema de archivos

Hugo Francisco González Robledo
hugo.gonzalez@upslp.edu.mx

presenta:

Agenda

- ¿Que es la encriptación?
- ¿Para que utilizarla?
- Software relacionado
- Usando particiones encriptadas
  - LUKS
  - dm-crypto
- Receta para encriptar una partición
  - Para usar un archivo como llave
- Tips para encriptar todo el sistema

¿Que es la encriptación?

- Al no haber definición, tomamos la definición relacionada de **Criptografía**[1]
- Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

1. Fuente : http://es.wiktionary.org/wiki/criptograf%C3%ADa

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

¿Para que la quiero utilizar?

- **Mantener oculta o protegida mi información**

por ejemplo

- Guardar los documentos importantes
- Guardar las fotos comprometedoras
- Guardar el pr0n
- Guardar mis contraseñas y llaves de acceso
- Por ser PARANOICO
- Por seguridad de mi información

Software relacionado

- GnuPG

- GnuPG es un reemplazo completo y libre para PGP. Debido a que no utiliza el algoritmo patentado IDEA , puede ser utilizado sin restricciones. GnuPG es Software Libre .
- http://www.gnupg.org/index.es.html

Software Relacionado

- GnuPG (GPG) se puede utilizar para cifrar correo, documentos, o realizar firmas de archivos. Incluso pudes cifrar comunicaciones de mensajeria :)
- Incluso podrías usar tus tarjetas smartcard!!!
- No es eficiente para cifrar una partición de tu sistema ...

Usando particiones encriptadas

- Usaremos LUKS y dm-crypt para manejar de forma transparente las particiones en nuestro sistema linux
- La ventaja de esto es que se puede hacer en cualquier distro
- Desventaja?: Necesitas kernel 2.6
- Se puede obtener todo con el paquete cryptsetup (antes cryptsetup-luks)

LUKS (Linux Unified Key Setup)

- *LUKS is the upcoming standard for Linux hard disk encryption. By providing a standard on-disk-format, it does not only facilitate compatibility among distributions, but also provide secure management of multiple user passwords. In contrast to existing solution, LUKS stores all setup necessary setup information in the partition header, enabling the user to transport or migrate his data seamlessly.*
- Extraido de : http://luks.endorphin.org/

dm-crypt

- *A new cryptographic device-mapper target for Linux kernel 2.6 which enables filesystem encryption.*
- Extraido de: http://www.saout.de/tikiwiki/tiki-index.php

- Device-mapper is a new infrastructure in the Linux 2.6 kernel that provides a generic way to create virtual layers of block devices that can do different things on top of real block devices like striping, concatenation, mirroring, snapshotting, etc... The device-mapper is used by the LVM2 and EVMS 2.x tools.
- dm-crypt is such a device-mapper target that provides transparent encryption of block devices using the new Linux 2.6 cryptoapi. The user can basically specify one of the symmetric ciphers, a key (of any allowed size), an iv generation mode and then he can create a new block device in /dev. Writes to this device will be encrypted and reads decrypted. You can mount your filesystem on it as usual. But without the key you can't access your data.

Encriptando archivos vs particiones

- Encriptar archivos es bueno, pero lo tienes que hacer archivo por archivo
- Al encriptar una partición, (recuerdan sistemas operativos) tienes un pedazo de disco, con archivos y directorios dentro que permanecen encriptados (y seguros)

Receta para encriptar una partición

- La siguiente receta se puede aplicar para encriptar una partición, o varias particiones con diferente “frase de paso”
- Esta receta (como las buenas) se puede modificar para adaptarla a tus gustos
- También vamos a ver como evitar tener que escribir la contraseña cada vez que montamos una partición

Paso 0

- Instalar las herramientas necesarias, en debian o ubuntu

```
# sudo apt-get install cryptsetup
```

Paso 1 (a) Opcional

- Verificar el disco en busca de errores ...

```
# /sbin/badblocks -c 10240 -s -w -t random -v /dev/sdc
(wait several hours...)
Checking for bad blocks in read-write mode
From block 0 to 295360984
done
Reading and comparing: done
Pass completed, 0 bad blocks found.
```

- Aparte de asegurarnos que el disco es usable, llenamos la partición con información aleatoria

Paso 1 (b) Opcional

- Llenar el disco con datos aleatorios (de manera directa)

```
# dd if=/dev/urandom of=/dev/sdc
(wait several hours...)
```

Paso 2

- Particionar el disco duro
- Importante asegurarse de las rutas, el particionamiento es un proceso destructivo

```
# /sbin/fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or
OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.
```

Paso 3

- Crear un mapeo entre el dispositivo lógico y el físico

```
# /usr/bin/cryptsetup --verbose --verify-passphrase create sdc1
/dev/sdc1
Enter passphrase: (enter your passphrase, and write it down
somewhere!)
Verify passphrase: (repeat passphrase)
#
```

El dispositivo físico será : /dev/disco

El dispositivo lógico será: /dev/mapper/disco

Paso 4

- Crear el sistema de archivos en la partición lógica

```
# /sbin/mkfs.ext3 -m 1 -O dir_index,filetype,sparse_super /dev/mapper/sdc1
(wait several minutes...)
mke2fs 1.35 (28-Feb-2004)
Filesystem label=
OS type: Linux
```

Paso 5

- Montar el sistema de archivos

```
# mkdir /home4
# mount /dev/mapper/sdc1 /home4
```

Paso 6

- Montar y desmontar en el futuro
  - Montar

```
# cryptsetup create sdc1 /dev/sdc1
# mount /dev/mapper/sdc1 /home4
```

  - Desmontar

```
# umount /home4
# cryptsetup remove sdc1
```

Resultado

- Tenemos nuestra(s) particiones en el sistema, cada que queramos usarlas tenemos que usar solamente el paso 6, montar o desmontar la partición.
- Cuando la desmontemos no hay problema, pero al montarla necesitamos introducir nuevamente la contraseña elegida ...

Usar un archivo como contraseña

- Algunas veces es “más seguro” usar una llave en lugar de una contraseña o frase ... (almacenarla en un lugar seguro.
- Creamos la llave (una forma)

```
#dd if=/dev/random of=/path/to/key/llave.key bs=1 count=256
```

- Modificar la creación del dispositivo añadiendo la ruta de la llave.
- Al mapear el dispositivo usamos el modificador

--key-file /path/to/key/llave.key

Para encriptar todo el sistema

- Podemos encriptar todo nuestro sistema ...
- menos /boot (partición de donde arranca)
- Si almacenamos nuestra llave en una USB, asegurarnos que tenemos soporte para USB y para dm-crypt desde el arraque, en el kernel y no como módulos :)
- crear el archivo /etc/crypttab y ligamos las particiones con el archivo llave

  var /dev/hda2 /media/flash/var.key

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Preguntas ???

- Contactar al autor en el correo :

hugo.gonzalez@upslp.edu.mx

- Revisar la documentación y faq de dm-crypto

http://www.saout.de/tikiwiki/tiki-index.php

Gracias por su atención

(y al expositor)