```
auth required pam_ecryptfs.so
```

Ahora, si se sale de la sesión y vuelve a entrar, podrá ver que el directorio *secret/* se ha montado automáticamente. Luego (si se desea) puede repetirse el proceso completo con otra clave para otro directorio.

Es posible cifrar el directorio home completo (en vez de tener que crear un usuario nuevo), pero es un proceso algo más complicado. Véase la entrada en el blog de Dustin Kirkland para más información [2].

Aumentando la Seguridad

La clave que utiliza eCryptfs para montar el directorio se almacena en *~/.ecryptfs/wrapped-passphrase* y se cifra utilizando un algoritmo de criptografía de clave simétrica mediante la contraseña de la cuenta de usuario. Por defecto, la clave consiste en un número de 128 bits generados aleatoriamente (difícil de recordar y difícil de adivinar). Cuando monta su directorio eCryptfs, se carga (*salted* y *hashed*) en el depósito de claves del núcleo. Si también se están cifrando los nombres de ficheros, se utiliza una segunda clave y también se carga en el depósito de claves del núcleo. Estas claves se utilizarán cada vez que se vaya a acceder a un fichero del directorio cifrado.

Esto se conoce como criptografía de dos factores: hace falta *tanto* el fichero *wrapped-passphrase como* la contraseña del usuario para acceder a los datos cifrados. Por otro lado, se puede configurar para que apunte a algún medio extraíble y de este modo desconectarlo de la máquina cuando no se tenga que ir. Para incrementar la seguridad, puede almacenar este fichero en una memoria USB en vez de en un disco duro, de modo que si alguien le robase el portátil, también tendría que robarle la clave. Para ello hay que crear el siguiente enlace *~/.ecryptfs/wrapped-passphrase* de modo que apunte al fichero que se encuentre en el medio extraíble. (Para mayor seguridad póngale un nombre poco obvio).

Téngase en cuenta que hay que añadir una línea a */etc/fstab* de modo que el medio extraíble siempre se monte en el mismo directorio:

```
/dev/sdb1 /media/usbkey ➥
ext3 defaults 0 0
```

Ahora es más importante que nunca almacenar la clave en algún otro lugar – las memorias USB son prácticas pero ¡se pierden fácilmente!

También puede probarse la opción *-w* para *ecryptfs-setup-private*, la cual utiliza una contraseña diferente (no la usada en el login) para proteger la clave. Esta opción es potencialmente más segura (un atacante tendría que adivinar dos contraseñas), pero no se podrá montar el directorio de forma automática.

Realizando una Copia de Seguridad de los Datos

Se puede realizar fácilmente una copia de seguridad de los datos cifrados desmontando el directorio y utilizando alguna herramienta para realizar copias de seguridad. Los ficheros se copiarán cifrados y podrá acceder a ellos con la clave correspondiente tal y como si fueran los originales. No podrá acceder a ellos sin la clave. No hace falta realizar nada más para proteger sus datos. Sin embargo, hay que recordar que si pierde el fichero con la clave (u olvida la contraseña), será incapaz de acceder a los datos. Una vez más, realice una copia de seguridad del fichero con la clave y manténgalo en un lugar seguro.

eCryptfs y Directorios del Sistema

Debería también tenerse en cuenta que a veces los datos sensibles se pueden escribir en otros directorios distintos al directorio personal, por ejemplo */tmp*.

Por ello, debería considerarse la configuración de la máquina de modo que se use eCryptfs para otros directorios, siempre dependiendo de los posibles datos sensibles que maneje.

Esto se puede realizar de la misma manera que se ha comentado anteriormente para el cifrado manual de directorios. Hay que asegurarse de que se deben añadir las líneas correspondientes a */etc/fstab* de modo que los usuarios que no sean root puedan montar los directorios relevantes.

Si ya posee datos en estos directorios, el proceso es algo más complicado que si se crea un directorio desde cero. Primero haga una copia de los datos del directorio y luego siga los siguientes pasos:

1. Cree el directorio nuevo. Debería tener temporalmente un nombre diferente. Configúrelo como se ha comentado anteriormente.
2. Móntelo y copie todos los ficheros del directorio antiguo al nuevo (¡incluyendo los ocultos, los que comienzan con un punto!)
3. Renombre el directorio antiguo (por ejemplo a */directorio_bk*) y desmonte el directorio cifrado.
4. Renombre el nuevo directorio, edite de forma adecuada */etc/fstab* y vuélvalo a montar.

Ahora sus datos deberían estar cifrados. Mantenga el directorio antiguo como copia de respaldo hasta asegurarse de que todo funciona correctamente. En el caso del directorio */tmp*, tendría más sentido borrar todos los datos temporales, borrar el directorio y volverlo a crear como un directorio cifrado.

También se puede configurar la swap para que se encuentre cifrada. Cifrarla implica que dejen de funcionar los modos de hibernación y de suspensión (actualmente Ubuntu se encuentra trabajando en la resolución de este problema), pero se asegurará de que no anden por la swap copias de los ficheros descifrados (otra opción, si posee bastante memoria en el sistema, consiste en desactivar la swap).

Para cifrar su partición de swap hay que instalar *cryptsetup*, y luego ejecutar *sudo ecryptfs-setup-swap*, que desmontará la partición de swap, la cifrará y la volverá a montar.

Desafortunadamente, aunque se añade una nueva entrada en */etc/fstab* automáticamente, la entrada antigua no se elimina. Habrá que editar manualmente el fichero */etc/fstab* (como root) y eliminar la entrada antigua de la swap. La nueva entrada de la swap se identificará como */dev/mapper/cryptswap* – esta es la línea de swap que hay que conservar.

Más Información

Para obtener información actualizada sobre eCryptfs y tutoriales de ayuda (que he utilizado en la redacción de este artículo), visite el blog de Dustin Kirkland [3]. ■

RECURSOS

[1] eCryptfs: *https://launchpad.net/ecryptfs*

[2] Migrando a un directorio home cifrado: *http://blog.dustinkirkland.com/2009/06/migrating-to-encrypted-home-directory.html*

[3] Blog de Dustin Kirkland: *http://blog.dustinkirkland.com*