Cifrado a Nivel de Ficheros con eCryptfs

Lugares Ocultos

eCryptfs cifra los datos de manera transparente, proporcionando una protección extra frente a posibles ladrones o intrusos espontáneos. **POR JULIET KEMP**

ECryptfs [1] ofrece cifrado a nivel de ficheros de tipo PGP para Linux (Figura 1). Cada vez que se escribe un fichero en un directorio cifrado con eCryptfs en el disco duro, lo cifrará automáticamente; cada vez que se lea un fichero de ese directorio, eCryptfs automáticamente lo descifrará. Este proceso ocurre en segundo plano y la configuración por defecto utilizará la contraseña de inicio de sesión del usuario para almacenar la clave de cifrado, haciendo que el proceso completo sea sencillo y automático cada vez que se inicie una sesión.

Una de las ventajas del cifrado a nivel de ficheros, al contrario que el cifrado basado a nivel de bloques (el sistema de ficheros completo) que proporcionan otras herramientas de criptografía, es que se pueden poseer varias claves en el mismo sistema. Esto significa que los usuarios en el mismo sistema pueden cifrar sus propios datos de manera individual y de forma separada; o un simple usuario puede cifrar directorios diferentes o incluso ficheros diferentes de forma separada. Los distintos usuarios pueden incluso utilizar el mismo directorio con diferentes claves, y cada usuario podrá descifrar sólo sus propios ficheros cifrados.

Configurando eCryptfs

Si está instalando Ubuntu desde cero, en el proceso de instalación se le preguntará al usuario si desea cifrar su directorio home como parte de este proceso de instalación. También se puede crear fácilmente un usuario nuevo con un directorio home cifrado (puede que tenga que instalar primero el paquete *cryptfs-utils*) con el siguiente comando:

```
sudo adduser --encrypt-home newusername
```

Desafortunadamente, este comando sólo funciona en Ubuntu; aunque Debian soporta eCryptfs, por ahora no soporta la opción *–encrypt-home* del comando *adduser*, ni tampoco la creación de directorios home cifrados en el proceso de instalación. Afortunadamente, si tiene un sistema con Debian o si ya posee un sistema Ubuntu en funcionamiento y no desea crear un usuario nuevo sólo para disponer de esta opción, puede instalarse y configurarse por sí mismo eCryptfs:

```
sudo apt-get install ecryptfs-utils ecryptfs-setup-private
```

Este comando crea un directorio *~/Private* y lo configura como cifrado. Cuando salga de su sesión, el directorio se almacenará como *~/.Private*, y cuando vuelva a iniciarla de nuevo, automáticamente se montará como *~/Private*. Su contraseña de usuario (de inicio de sesión) se utiliza para almacenar su clave de cifrado. Es mejor dejar que eCryptfs genere una de forma aleatoria (una clave aleatoria es mucho más difícil de romper que una proporcionada por el usuario). Sería una idea muy buena almacenar la clave en algún lugar separado, en caso de desastre (o que se le olvide su contraseña de inicio de sesión). Para conseguirla ejecute el siguiente comando:

```
ecryptfs-unwrap-passphrase .ecryptfs/wrapped-passphrase
```

Ahora ya puede elegir los directorios que desee cifrar: sólo hay que moverlos a *~/Private* y crearles un enlace simbólico en su lugar original. Por ejemplo, para mover el directorio *.ssh*, teclee los siguientes comandos:

```
cd
mv .ssh Private/
ln -s Private/.ssh .ssh
```

Cuando cierre su sesión (o desmonte *Private*), tanto el contenido de estos directorios como los nombres de ficheros quedarán cifrados, de modo que ningún usuario del sistema podrá identificar lo que tenga en este directorio. Al mover un directorio al directorio cifrado, lo cifra automáticamente.

Si no desea que se monte de forma automática el directorio *Private* cuando inicie la sesión, borre *~/.ecryptfs/auto-mount* (y *~/.ecryptfs/auto-umount*). Son dos fiche-