ros vacíos, de modo que para crearlos de nuevo, simplemente bastará con hacerles un *touch* y se volverán a montar de forma automática. Tenga en cuenta que si mueve directorios o ficheros importantes a *Private*, puede que le aparezcan errores en el inicio de sesión, especialmente si mueve algún fichero relacionado con el escritorio.

Cifrando un Directorio Manualmente

Si no desea que su directorio cifrado sea *~/Private*, o si necesita un segundo directorio cifrado (quizás con una clave diferente), puede crear manualmente un directorio cifrado en un lugar diferente:

```
mkdir ~/secret
chmod 700 ~/secret
sudo mount -t ecryptfs➥
secret secret
```

El sistema pedirá que se introduzca una cifra y un tamaño de clave (si no se encuentra familiarizado con las opciones, simplemente puede quedarse con los valores por defecto).

También le preguntará si desea activar la opción de *paso de texto plano*, la cual permite a los ficheros que no sean de eCryptfs ser leídos y escritos dentro de un punto de montaje eCryptfs. Esta opción puede ser útil en algunas situaciones, pero tiene como inconveniente principal que no se tendrá la seguridad total de que todos los ficheros del directorio se encuentren protegidos. Se encuentra desactivada por defecto, que normalmente es la mejor apuesta.

El cifrado de los nombres de los ficheros es exactamente lo que su nombre indica: se cifran simultáneamente los nombres de los ficheros y sus contenidos, de modo que sólo el propietario puede ver los nombres de los ficheros que se encuentren dentro del directorio cifrado y sólo cuando se monte con eCryptfs. Lo mejor es activarlo (no se activa por defecto).

A continuación se solicitará la contraseña. Como esta es la primera vez que se utiliza este punto de montaje, el sistema mostrará un aviso de que no se ha utilizado anteriormente esta contraseña. También preguntará si desea almacenarla (en el depósito de claves raíz) para evitar este aviso en el futuro.

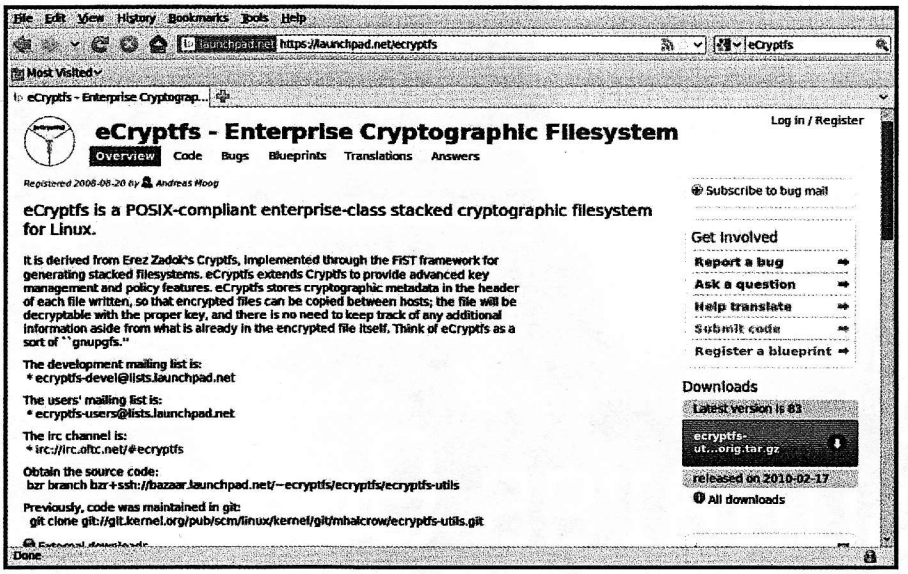

Figura 1: eCryptfs se encuentra en el sitio Launchpad. El responsable Dustin Kirkland trabaja para Canonical, el patrocinador de Ubuntu.

En los argumentos de *mount*, la primera ruta es el directorio que se está montando con eCryptfs y la segunda ruta es el punto de montaje eCryptfs. Estas opciones pueden ser diferentes, pero montarlo en el mismo punto significa que los ficheros del directorio cifrado siempre *serán* accesibles por eCryptfs. También hará que todo el proceso sea transparente.

Una vez que haya terminado de usar este directorio, se puede desmontar. Si intenta ahora mirar los ficheros contenidos en él, podrá ver una larga cadena cifrada como nombre de fichero (suponiendo que se haya activado la opción de cifrar los nombres de ficheros), y si mira los contenidos, aparecerán como ficheros binarios.

Hay un par de desventajas relacionadas con el cifrado manual de los directorios. Una de ellas es que hay que introducir las opciones de cifrado cada vez que se monte el directorio. Estas opciones se pueden pasar por la línea de comandos de la siguiente forma:

```
sudo mount -t ecryptfs secret/ secret/ ➥
-o ecryptfs_cipher=aes,➥
ecryptfs_key_bytes=16,➥
ecryptfs_passthrough=n
```

Desafortunadamente no hay ningún parámetro de la línea de comandos que permita cifrar los nombres de los ficheros. Téngase en cuenta que se puede montar el mismo directorio con y sin el cifrado de los nombres de ficheros en ocasiones diferentes sin ningún tipo de problema.

La otra desventaja es que hay que ser usuario root para montar este directorio. Para solucionar este problema, hay que montar el directorio como root, luego mirar el fichero */etc/mtab* para obtener las opciones y, a continuación, añadirle *user*. La línea resultante, que deberá parecerse a la mostrada en el Listado 1, hay que añadirla a */etc/fstab*. Luego se desmonta el directorio con *sudo umount /secret*.

Ahora hay que añadir manualmente la clave al depósito de claves del usuario con *ecryptfs-manager*. Elija la opción 1 (*add passphrase key to keyring*) y teclee su contraseña, luego con la opción 4 se sale. Teclee *mount -i newsecret* (la opción *-i* evita que se invoque el asistente de mount), y ahora ya se podrá utilizar el directorio cifrado. Tras desmontarlo, se usa el comando *keyctl clear @u* para borrar el depósito de claves de la sesión.

Con dos pasos más se puede conseguir que todo esto se realice de forma automática en el inicio de sesión. Primero, hay que añadir la línea *mount -i secret* a *~/.bashrc*. Luego, hay que añadir a */etc/pam.d/login* la siguiente línea:

Listado 1: Añadir a /etc/fstab

```
/home/juliet/secret /home/juliet/secret ecryptfs user,rw,
ecryptfs_sig=9ffdcd5087c0c049,ecryptfs_fnek_sig=9ffdcd5087c0c049,\
ecryptfs_unlink_sigs,ecryptfs_cipher=aes,ecryptfs_key_bytes=16 0 0
```