Criptare „manager proof”

Ovidiu Constantin
ovidiu@mybox.ro
http://blog.mybox.ro/

Situația

- În companie există manageri și alți "mobile warriors" (sales, consultanți)

- Au date importante/confidențiale pe notebook-uri mici și scumpe

- Acestea pot fi pierdute sau furate ușor

Cerințe

- Ușor de instalat pe un sistem deja existent
- Fără să necesite parole suplimentare sau rularea de programe
- Backup/restore simple și sigure
  - Fișierele să rămână criptate în backup
  - Să se poată folosi sistemul de backup deja existent

Soluția

eCryptfs - https://launchpad.net/ecryptfs

- Există suport în kernel de la 2.6.19
- Criptare la nivel de filesystem
- Permite criptarea selectivă a fișierelor
- Integrare cu PAM pentru mount/umount automat

Exemplu de implementare

- Ubuntu montează ~/.Private în ~/Private
- Se mută fișierele sensibile în ~/Private
- Se crează symlink-uri către noua locație
- Ușor de securizat documentele și fișierele de configurare

Instalare

```
root@apollo:~# aptitude search ecryptfs-utils
i   ecryptfs-utils                          - ecryptfs cryptographic filesystem (utilities)
root@apollo:~# su - test
test@apollo:~$ ecryptfs-setup-private
Enter your login passphrase:
Enter your mount passphrase [leave blank to generate one]:
Enter your mount passphrase (again):

************************************************************************************
YOU SHOULD RECORD YOUR MOUNT PASSPHRASE AND STORE IT IN A SAFE LOCATION.
  ecryptfs-unwrap-passphrase ~/.ecryptfs/wrapped-passphrase
THIS WILL BE REQUIRED IF YOU NEED TO RECOVER YOUR DATA AT A LATER TIME.
************************************************************************************


Done configuring.

Testing mount/write/umount/read...
```

Utilizare

```
test@apollo:~$ mount | grep ecryptfs
/home/ovidiu/.Private on /home/ovidiu/Private type ecryptfs (ecryptfs_sig=7[illegible]a,ecry
ptfs_fnek_sig=4[illegible],ecryptfs_cipher=aes,ecryptfs_key_bytes=16)
/home/test/.Private on /home/test/Private type ecryptfs (ecryptfs_sig=1[illegible],ecryptfs
_fnek_sig=[illegible],ecryptfs_cipher=aes,ecryptfs_key_bytes=16)
test@apollo:~$ ls -la
total 20
drwxr-xr-x 5 test test 4096 2010-02-11 14:38 .
drwxr-xr-x 4 root root 4096 2009-11-15 00:44 ..
drwx------ 2 test test 4096 2010-02-11 14:38 .ecryptfs
drwx------ 2 test test 4096 2010-02-11 14:38 Private
drwx------ 2 test test 4096 2010-02-11 14:38 .Private
test@apollo:~$ echo "Ho-ho-hoooo" > ~/Private/test.txt
test@apollo:~$ cat ~/Private/test.txt
Ho-ho-hoooo
test@apollo:~$ ls -lR ~/.Private/
/home/test/.Private/:
total 12
-rw-r--r-- 1 test test 12288 2010-02-11 14:39 ECRYPTFS_FNEK_ENCRYPTED.FWaH8c3a.RYwmETDk5Hhbav9I
3F09ahLs.tY28y3RyggxqXSNkC37cXTtU--
test@apollo:~$ cat ~/.Private/ECRYPTFS_FNEK_ENCRYPTED.FWaH8c3a.RYwmETDk5Hhbav9I3F09ahLs.tY28y3R
yggxqXSNkC37cXTtU--

{3G2p[
```

Atacuri eșuate

```
root@apollo:~# su - test
keyctl_search: Required key not available
Perhaps try the interactive 'ecryptfs-mount-private'
test@apollo:~$ ls -l ~/Private/
total 0
test@apollo:~$ logout
keyctl_search: Required key not available
Perhaps try the interactive 'ecryptfs-mount-private'
```

Atacuri eșuate (2)

```
root@apollo:~# passwd test
Introduceți noua parolă UNIX:
Retastați noua parolă UNIX:
passwd: parolă actualizată cu succes
root@apollo:~# ssh test@localhost
test@localhost's password:
Linux apollo 2.6.31-19-generic #56-Ubuntu SMP Thu Jan 28 01:26:53 UTC 2010 i686

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/

14 packages can be updated.
3 updates are security updates.

Last login: Thu Feb 11 14:47:37 2010 from localhost
test@apollo:~$ ls -l Private/
total 0
test@apollo:~$ ecryptfs-mount-private
Enter your login passphrase:
Error: Unwrapping passphrase and inserting into the user session keyring failed [-5]
Info: Check the system log for more information from libecryptfs
ERROR: Your passphrase is incorrect
Enter your login passphrase:
```