

Putting it all together on Fedora Core 5 – Clint Tinsley

Towards the end of the presentation, Robert demonstrated the burning of a CD as raw data which he called "Security through obscurity". During the presentation, Robert also showed how to create a file as a partition as a loopback device and use it as an encrypted partition mounted as a folder which is very handy if you don't have any available logical partitions available on your hard drive for encryption. Taking these concepts and applying them on FC5, I found that I could create a huge file, 650 megabytes - just the right size for burning to CD, and make it an encrypted device. Unlike Ubuntu, FC5 comes with all the tools so no updates or downloads were necessary to get dm-crypt to work.

Following the steps below, I created my encrypted folder at /mnt/vault and stored a VMware virtual machine in it that I could run from VMware successfully. Then I removed encrypted folder including the loopback file so all I had was my original file, basically a garbage file if you tried to look inside it, unusable, unrecognizable data. Proof of concept was to burn that file to a CD, destroy the original file, copy the file from the CD back to my home directory, and go through the steps necessary to get remounted in its unencrypted state so I could run the virtual machine again. The steps I took (as root):

1) Create a 650MB file in my home directory.

```
dd if=/dev/urandom of=/home/tinsleyc/vault bs=1MB count=650
```

2) `chown tinsleyc:tinsleyc /home/tinsleyc/vault`

I was root when I did this and I need to be the owner of the file to burn it and restore it from CD.

3) `losetup /dev/loop0 /home/tinsleyc/vault`

4) `cryptsetup -y create myvault /dev/loop0`

Note: You are assigning the permanent password to myvault in this step.

5) `dmsetup ls` (verify the existence of myvault as being created.)

6) `mkfs.ext3 /dev/mapper/myvault`

/dev/mapper/myvault is where cryptsetup makes its encrypted files and you need to format the file system in order to use it.

7) `mkdir /mnt/vault` - Need a mount point for my encrypted partition where I can access it unencrypted

8) `chown tinsleyc:tinsleyc /mnt/vault` - I need ownership of this because everything done so far is done as root.

9) `mount /dev/mapper/myvault /mnt/vault`

After I did all this, I created a virtual machine in /mnt/vault and ran it in VMware. Then I "destroyed" the encrypted partition:

1) `[root@vmware /]# umount /mnt/vault`

2) `[root@vmware /]# cryptsetup remove myvault`

3) `[root@vmware /]# losetup -d /dev/loop0`

4) `[root@vmware /]# rmdir /mnt/vault`

By doing the above, I have removed all traces of encrypted partition.

I burned the /home/tinsleyc/vault to CD using K3B with file after which, I deleted the original vault file and copied the vault file from the CD back to /home/tinsleyc. Then I performed the following (as root):

1) `[root@vmware /]# mkdir /mnt/vault`

2) `[root@vmware /]# chown tinsleyc:tinsleyc /mnt/vault`

3) `[root@vmware /]# losetup /dev/loop0 /home/tinsleyc/vault`

4) `[root@vmware /]# cryptsetup -y create myvault /dev/loop0`

Enter passphrase:

Verify passphrase:

(Using the same password/passphrase as when I originally created myvault originally.)

5) [root@vmware /]# mount /dev/mapper/myvault /mnt/vault

Done. Ran VMware again to access the Virtual machine located in /mnt/vault, success!

Proof of concept is that it all worked such that you could create a file up to 4 GB (or 8 GB for double layer DVDs) in size, mount it as an encrypted partition, put your data on it and then burn it to CD as a backup or for transportation to another computer and it would be completely encrypted. To restore it, you would have to know at least two things, the name of file created by cryptsetup (myvault) and the passphrase.

FC5 Resources:

Good HowTO -

<http://forums.fedoraforum.org/forum/showthread.php?t=88586>

A lot of links and cross-links to this web site!

<http://www.shimari.com/dm-crypt-on-raid/>

LUKS (FC5 Technology):

<http://www.saout.de/tikiwiki/tiki-index.php?page=EncryptHomeDirUsingLUKS>

<http://www.raoul.shacknet.nu/2005/11/10/encrypt-devices-using-dm-crypt-and-luks/>

<http://rpmfind.net/linux/RPM/fedora/5/i386/cryptsetup-luks-1.0.3-0.rc2.i386.html>

<http://luks.endorphin.org/about>

More to read...

<http://article.gmane.org/gmane.linux.kernel.device-mapper.dm-crypt/1811>

<http://www.redhat.com/archives/fedora-list/2006-March/msg02469.html>

<http://www.spinics.net/lists/dm-crypt/msg00108.html>

<http://www.spinics.net/lists/dm-crypt/msg00111.html>

TrueCrypt:

<http://www.schneier.com/blog/archives/2006/05/truecrypt.html>

<http://www.truecrypt.org/>