

Secure Encryption of a Flash Drive



- Anti Forensics

Use CryptSetup to use a different encryption other than the default in DM-Crypt.

Why?



If you use Ubuntu's device manager to encrypt your flash drive it will be using the default encryption AES with no extra protection.

With my tutorial you can use the Terminal to use a safer form of encryption one that is not known to have any flaws such as the normal AES.

Weakness?!



Could it be true that with a lot of device encryption programs out there are flawed in some way?

Well the encryption itself is sound but there is an attack where a hacker plants a large file into your encrypted drive while it is open then when he/she takes your drive they can run a program that will look for a large block the size of the file and start to compare a bunch of ways that that text could come from the original file.

Weakness?! Cont.



Think of it like a very complex algebra problem...

All your trying to do is find the correct y to make x .

- X is the encrypted output
- Y is the Key
- A is the big file you added
- $X=A+Y-255$

If the encryption key was 10, the big file you added is the value of 999999

So it goes to say that would be...

$$X=999999+10-255$$

- $X=999754$

Weakness?! Cont.



So to reverse that simple algorithm would be with the knowlage that you have (the big file)

$$Y=X-A+255$$

$$Y=999754-999999+255$$

$$Y=10$$

Now trying to find the key through that process for AES would be allot more complicated but still the same idea.

We can change the encryption type by a little to encrypt each section differently.

Tutorial





This is very simple really but it just takes some time to get down 100% then you will not need this tutorial.

-Open a Terminal (Ctrl+Alt+T)

Insert your flash drive, make sure you back up everything you want to keep on it, because this process will destroy all data that is currently on that Flash Drive.

-Now you need to find out what it has your FD stored as.

```
sudo fdisk -l
```

For me it was /dev/sdb

Now lets securely override everything that is on that drive.

```
sudo cryptsetup create FD /dev/sdb -d /dev/urandom
```

```
sudo badblocks -swt random /dev/mapper/FD
```

```
sudo cryptsetup remove FD
```

Now time for the fun stuff.

Now it is a time for you to choose on a encryption method. AES, Blowfish, Twofish, etc

Once you do that you need to decide on a key size 40, 128, 256, etc
I would recomend 256.



Once you have chosen all you need to you can continue, for this tutorial I will be using AES with a 256 bit key.

Now we can format the drive.

```
sudo cryptsetup -c aes-cbc-essiv:sha256 -h whirlpool -s 256 luksFormat /dev/sdb
```

Follow what it tells you to do, if you chose a different encryption than aes just replace the aes, so for twofish it would be twofish-cbc-essiv:sha256

The -s sets the key size option.

Now you need to open the luks device.

```
sudo cryptsetup luksOpen /dev/sdb FD
```

-Type in your password you made it with.

That will open a device mapping called FD in your mapper file. Now you need to give that mapping a filesystem.

```
sudo mkfs.ext2 /dev/mapper/FD
```

Now you need to make a temp folder to mount your encrypted device to.

```
mkdir tmp
```

```
sudo mount /dev/mapper/FD tmp
```



-Change the ownership of the device to your username.

```
sudo chown kenthefurry: tmp -R  
chmod 700 tmp -R
```

Now you can unmount and eject your device...

```
sudo umount tmp  
rmdir tmp  
sudo cryptsetup remove FD  
sudo eject /dev/sdb
```

Now all you have to do is take the flash drive out and put it back in.
Then type in your password and it will go through all the steps.

Secure Encryption of a Flash Drive



The End

By KenTheFurry

Email: KenTheFurry@gmail.com

GPG Key: 068ACDD2