

Linux Disk Encryption

Introduction to disk encryption in Linux
Jozi Linux User Group

Why encrypt?

- Laptops get stolen,
- Bypass BIOS locks by mounting drive in another box
- If box is rooted and data encrypted still safe
- Some confidence in data disposal when discarding

How to encrypt

- Linux 2.6.16 or better
- Overwrite disk with random data
 - `badblocks -c 10240 -s -w -t random -v /dev/sdb`
- Install “`apt-get install cryptsetup`”
- Create partitions
 - `fdisk /dev/sdb`

How to encrypt

- Setup LUKS
 - `Cryptsetup --verbose --verify-passphrase luksFormat /dev/sdb1`
- Choose a good pass phrase
- Assign a virtual device to the encrypted device
 - `Cryptsetup luksOpen /dev/sdb1 mydrive`
- Create a filesystem
 - `Mkfs.ext4 /dev/mapper/mydrive`

How to encrypt

- Mount the drive
 - Mount `/dev/mapper/mydrive /mnt`
- Unmount
 - `Umount /mnt`
 - `Cryptsetup luksOpen /dev/mapper/mydrive`

LUKS Features

- Key features that LUKS provides include:
 - Support for either passphrase or keyfiles as encryption keys
 - Per partition key creation and revocation
 - Multiple passphrases or keyfiles for a particular partition, up to 8

LuksSetup

- Cryptsetup options
 - -c defines the cipher type
 - -y prompts for password confirmation on password creation
 - -s defines the key size
 - “cryptsetup -c aes-xts-plain -y -s 512
luksFormat /dev/sda2”

Keyfile

- Can use keyfile to unlock encrypted volume.
 - Keyfile.passphrase -
 - Keyfile.randomtext -
 - `dd if=/dev/urandom of=mykeyfile bs=512 count=4`
 - Keyfile.binary
- “`cryptsetup -c <desired cipher> -s <key size> -v luksFormat /dev/<volume to encrypt> /path/to/mykeyfile`”

Keyfile

- Can have up to 8 keyfiles, passphrases per volume
 - `cryptsetup luksAddKey /dev/<encrypted volume> /path/to/mykeyfile`
- To mount directory at boot time make passphrase same as your password.
- Add `pam_mount.so`
- Edit `common-pammount`

pam_mount

Add to common-pammount

```
auth    required pam_mount.so  
use_first_pass
```

```
session required pam_mount.so  
use_first_pass
```

pam_mount

- Add @include common-pammount to /etc/pam.d/gdm,gdm-session,login
- Edit /etc/security/pam_mount.conf.xml
 - <volume fstype="crypt" path="/dev/sda3" mountpoint="/home" />