Chapter 22 Encrypting Disks - Notes

22.2 Introduction

Filesystems may be **encrypted** to protect them from both prying eyes and attempts to corrupt data they contain. Encryption can be chosen at installation, or incorporated later. Linux distributions most often use **LUKS** method, and perform encrcyption-related tasks using **cryptsetup**.

22.3 Learning Objectives:

- Provide sound reasons for using encryption and know when it is called for.
- Understand how **LUKS** operates through the use of **cryptsetup**.
- Set up and use encrypted filesystems and partitions.
- Configure the system to mount encrypted partitions at boot.

22.4 Why Use Encryption?

Encryption should be used whenever sensitive data is being stored and transmitted. Configuring and using block device level encryption provides one of the strongest protections against hard caused by loss or compromise of data contained in hard drives + other media.

Modern Linux distributions offer choice of encrypting all or some of disk partitions during installation. Also straightforward to create + format encrypted partitions at later time, but cannot encrypt already existing partition in place without data copying operation.

22.5 LUKS

Modern Linux distributions provide block device level encryption mainly through use of **LUKS** (**L**inux **U**nified **K**ey **S**etup). Using block device encryption highly recommended for portable systems such as laptops, tablets, smart phones.

LUKS installed on top of **cryptsetup**, powerful utility that can also use other methods such as **plain dm-crypt** volumes, **loop-AES**, **TrueCrypt**-compatible format. Won't discuss these alternatives, as LUKS (which was already designed for Linux, but also been exported to other operating systems) standard method most often used in Linux.

dm-crypt kernel module uses **device mapper** kernel infrastructure that is also heavily used by LVM, which will be discussed later.

Because LUKS stores all necessary information in partition header itself, rather easy to migrate partitions to other disks or systems.

LUKS can also be used to transparently encrypt swap partitions.

22.6 cryptsetup

Basically, everything done with Swiss army knife program **cryptsetup**. Once encrypted volumes set up, can be mounted/unmounted with normal disk utilities.

General form of command:

```
cryptsetup [OPTION...] <action> <action-specific>
```

and full listing of possibilities generated by:

```
$ cryptsetup --help
```

22.7 Using an Encrypted Partition

If partition `/dev/sdc12` already exists, following commands will set up encryption, make it available to LUKS, format it, mount it, use it, and unmount it.

First, need to give partition to LUKS:

```
$ sudo cryptsetup luksFormat /dev/sdc12
```

Will be prompted for passphrase that will need to open use of encrypted volume later. Note: only have to do this step once, when setting up encryption. Kernel may not support default encryption method used by **cryptsetup**. In such case, can examine `/proc/crypto` to see methods supported by system, and can supply method:

```
$ sudo cryptsetup luksFormat --cipher aes /dev/sdc12
```

Can make volume available at any time with:

```
$ sudo cryptsetup --verbose luksOpen /dev/sdc12 SECRET
```

where you will be prompted to supply passphrase. Can format partition:

```
$ sudo mkfs.ext4 /dev/mapper/SECRET
```

mount it:

```
$ sudo mount /dev/mapper/SECRET /mnt
```

and then use to heart's content, just as if it were an unencrypted partition. When done, unmount with:

```
$ sudo umount /mnt
```

and then remove mapper association for now. Partition will always be available for later use:

```
$ sudo cryptsetup --verbose luksClose SECRET
```

22.8 Mounting at Boot

To mount encrypted partition at boot, two conditions have to be satisfied:

1. Make appropriate entry in `/etc/fstab`. Nothing special about this, does not refer to encryption in any way. Can be as simple as:

```
/dev/mapper/SECRET /mnt ext4 defaults 0 0
```

2. Add entry to `/etc/crypttab`. Can be as simple as:

```
SECRET /dev/sdc12
```

Can do more in this file, such as specifying password if you don't want to be prompted at boot (which seems counterproductive security-wise). See **man crypttab** to find out what can be done with this file.

##

Back to top

Previous Chapter - Table of Contents - Next Chapter