Slackware ARM/Aarch64 Disk Encryption

Still a work in progress.

This article outlines how to install Slackware with disk encryption on the Pine64 Pinebook Pro. It should work on other Slackware ARM supported hardware models. It has not been tested on a Slackware 32-bit ARM install. The README_CRYPT.TXT in the root of your Slackware installation media and on your chosen Slackware mirror covers most of this in depth. However, there are some recommendations about software and hardware.

- A fresh full installation of Slackware ARM
- Strongly suggested that you **do not** use a SD Card as your root disk
- SD Card stores the unencrypted boot partition **only**

This guide focuses on LUKS + LVM storage **encryption to protect mobile hardware**.

It is highly recommended that you install a NVMe disk to your Pinebook Pro using the NVMe ribbon cable from Pine64. You can find other hardware recommendations within the Slackware Aarch64 or ARM installation documentation, here. Disk encrypt has been tested on the Raspberry Pi 4, RockPro64, and Pinebook Pro.

Partitioning

To keep this guide on topic it will cover a basic partition schema for the Pinebook Pro. Partitioning is mostly already covered on other pages of this wiki. The goal is to provide a simple example that can be modified for any configuration.

Make sure you do not overwrite important data when you encrypt your disk.

My drive was identified as /dev/nvme0n1 by the Slackware installer. I created a partition named /dev/nvme0n1p1. In this case I claimed the whole NVMe disk. A single partition that fills the whole disk needs to be created on it. I encrypted it with cryptsetup using a key size of 256. Be aware that disk could be identified differently on your system. Make sure you check the output of the “lsblk” command.

This is the partition table on my Pinebook Pro with the NVMe drive. Notice the eMMC was removed.

```
[ pbpro.local.lan ~ ] lsblk
NAME               MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINTS
mtdblock0           31:0    0    16M  0 disk
mmcblk1            179:0    0  14.8G  0 disk
```

```
└─mmcblk1p1        179:1    0  14.8G  0 part  /boot
nvme0n1            259:0    0 232.9G  0 disk
└─nvme0n1p1        259:1    0 232.9G  0 part
  └─luksnvme0n1p1  252:0    0 232.9G  0 crypt
    ├─cryptvg-swap 252:1    0     4G  0 lvm   [SWAP]
    └─cryptvg-root 252:2    0 228.9G  0 lvm   /
```

Run the cryptsetup command and encrypt the partition.

```
cryptsetup -s 256 -y luksFormat /dev/nvme0n1p1
```

You will be asked for a password by cryptsetup. Keep this password in a safe place. Additionally, make sure it is a strong password. The next step requires the disk be unlocked. Use cryptsetup once more like so:

```
cryptsetup luksOpen /dev/nvme0n1p1 luksnvme0n1p1
```

The partition table is similar to what is recommended in the Slackware ARM Pinebook Pro installation documentation. The swap and root partition on located in the LVM + LUKS schema.

Initializing LUKS and LVM

Other methods of disk encryption will work similarly. This guide will focus on LUKS + LVM storage encryption to protect mobile hardware. The following is modified directions from the README_CRYPT.TXT found here .

Create the physical volume and volume group:

```
pvcreate /dev/mapper/luksnvme0n1p1
```

Create the volume group:

```
vgcreate cryptvg /dev/mapper/luksnvme0n1p1
```

Create a 4GB logical volume that will store the swap partition:

```
lvcreate -L 4G -n swap cryptvg
```

Allocate the remaining space in the volume group to your root partition:

```
lvcreate -l 100%FREE -n root cryptvg
```

You can now format your swap partition:

```
mkswap /dev/cryptvg/swap
```

Installation

Launch the Slackware installer:

```
setup
```

The full installation process is not covered to remain on-topic. If you require assistance with the installation process, see here. You can also get help on the LinuxQuestions.org forums.

Tips

Be certain you select the correct root disk (/dev/cryptvg/root) and the swap partition (/dev/cryptvg/swap) and answer all the questions until the installer is finished. The Slackware installer handles formatting and mounting the storage devices. The SD Card will be mounted as /boot automatically.

Exit the installer by **launching a shell**.

DO NOT REBOOT!

Post Installation: The boot loader

Your system will be unable to boot if you shut it down before updating the boot loader configuration. Enter a chroot shell and point the boot loader to your encrypted root disk and LUKS block device.

Enter a chroot:

```
chroot /mnt
```

Edit the boot loader configuration file:

```
nano /boot/extlinux/extlinux.conf
```

Notice the file syntax and edit the APPEND line within the file like so:

```
APPEND rootfs=ext4 root=/dev/cryptvg/root luksdev=/dev/nvme0n1p1
```

Make sure you adapt **rootfs** to use the file system of your root disk. For example, f2fs, ext3, btrfs, etc. You may also need to edit the “root” variable and the “luksdev” variable to accommodate differences on your system. Point luksdev to your encrypted block device. Set root to your decrypted disk volume.

Make sure you save and close the extlinux.conf boot loader configuration.

Exit the chroot shell by typing “exit” and shut down the system completely by typing “poweroff”.

You can now restart your Slackware system.

Additional Information

Future revisions of this guide will include the process of using an encrypted swap partition, home partition, or both combined. A section could also be added to use an encrypted file mounted as a loop back device on an unencrypted file system. Quite useful on systems where you have root, but you cannot add disk encryption to the root disk or swap.

Known Issues

- This issue has been addressed. ~~The serial console does not display the password prompt to decrypt storage.~~

~~The Pinebook Pro has a monitor that remedies this. However, the RockPro64, Raspberry Pi 3/4, will require a display to be attached. This makes it difficult to use a headless system. As a workaround, you can boot your system and decrypt the disk with a key file. You can store the key file on the SD Card. When you want to leave your system encrypted you can simply remove the SD card and take it with you.~~

- The Pinebook Pro does not always restart properly when the “reboot” command is used. This is marked as a known issue. ~~It is unclear if this is due to the disk being encrypted.~~

A workaround is to run the “poweroff” command to completely shut down the system instead. Then power it back up with the power button.

Sources

* Originally written by Brenton Earl

howtos, arm, aarch64, storage, LUKS, LVM, encryption