Section Overview

What You Will Learn

- Physical security threats.
- When you have control over physical security.
- Third party physical security.
- Cloud security.
- Strategies to mitigate physical security risks.
- Data encryption.

Physical Security

Physical Security Is Linux Security

- Physical access poses a great security threat to your Linux system!
- Single user mode.
    - Allows unrestricted access.
- Only allow physical access when necessary.

Physical Security Guidelines

- Keep your system away from attackers!

Systems Under Your Control

- Deep the data center and computer rooms locked at all times.
    - Keep unauthorized personnel from entering.
- Maintain access controls.
- Limit access to each individual room.
- Keep servers in locked server rooms.

Visitors

- Allow access by need.
- Escort visitors.
- Log visits.

UNITED STATES DEPARTMENT OF AGRICULTURE
ANIMAL AND PLANT HEALTH INSPECTION SERVICE

DATA CENTER VISITOR LOG

YEAR	DATA CENTER LOCATION	NAME OF DATA CENTER MANAGER	IN THE EVENT OF AN EMERGENCY, CONTACT THE DATA CENTER MANAGER AT OR .

DATE	VISITOR NAME (*LAST, FIRST, MI*)	VISITOR SIGNATURE	ORGANIZATION	FORM OF IDENTIFICATION	PURPOSE OF VISIT	AUTHORIZED ESCORT	TIME	
							IN	OUT
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM
							AM PM	AM PM

Systems Not Under Your Control

- Data centers / colos
  - Like “banks” of data.
  - Possible targets for attackers
  - Needs processes, procedures, and controls in place to protect your valuable data.

Data Centers

- Access controls
  - Security guards, gates, checkpoints.
  - Video surveillance systems.
  - Alarm systems.
  - Multifactor authentication systems.
  - Access policies, including revoking access.
  - Photo ID badges.
  - Background checks on employees.

https://www.flickr.com/photos/chrisdag/865711871

DATA CENTER
DATA CENTER

Cloud

- At some point the cloud is real equipment.
- Physical security is still important.
- Your data is on their storage systems.
  - The provider has access to your virtual disks.
  - If encryption is available, use it.

Protecting Linux Against Physical Attacks

Gaining Access to a Linux System

- Single User Mode
- Power Resets

Physical Security Demo

Single User Mode

and Blank Root Passwords

Securing the Boot Loader

Disk Encryption

Encryption

Unencrypted / Plaintext:

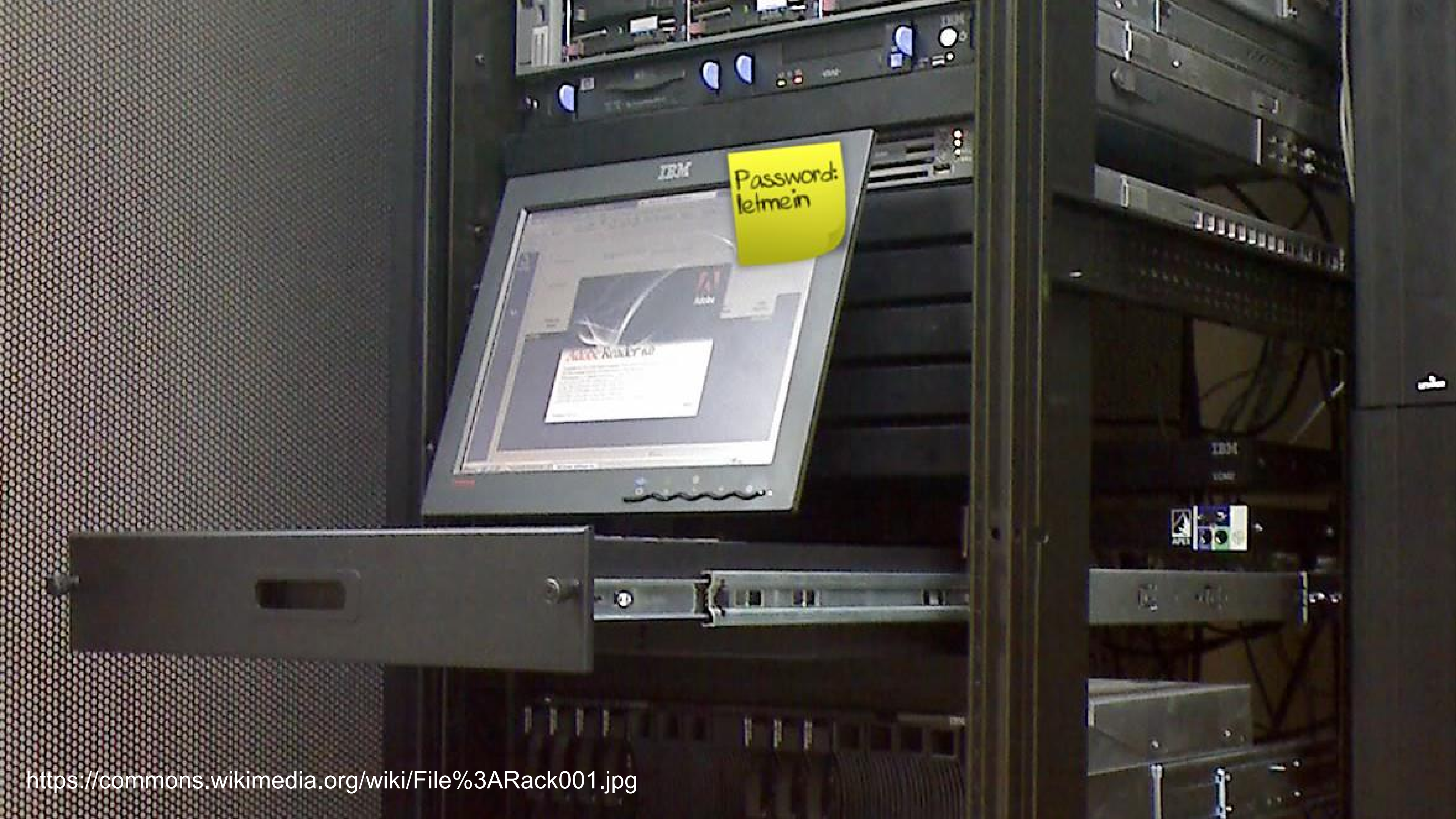
```
letmein123
```

Encrypted / Ciphertext:

```
$1$0vcWGUqX$bbo7e/Zohvj7.v94Mp0lV0
```

OS Needs Unencrypted Access

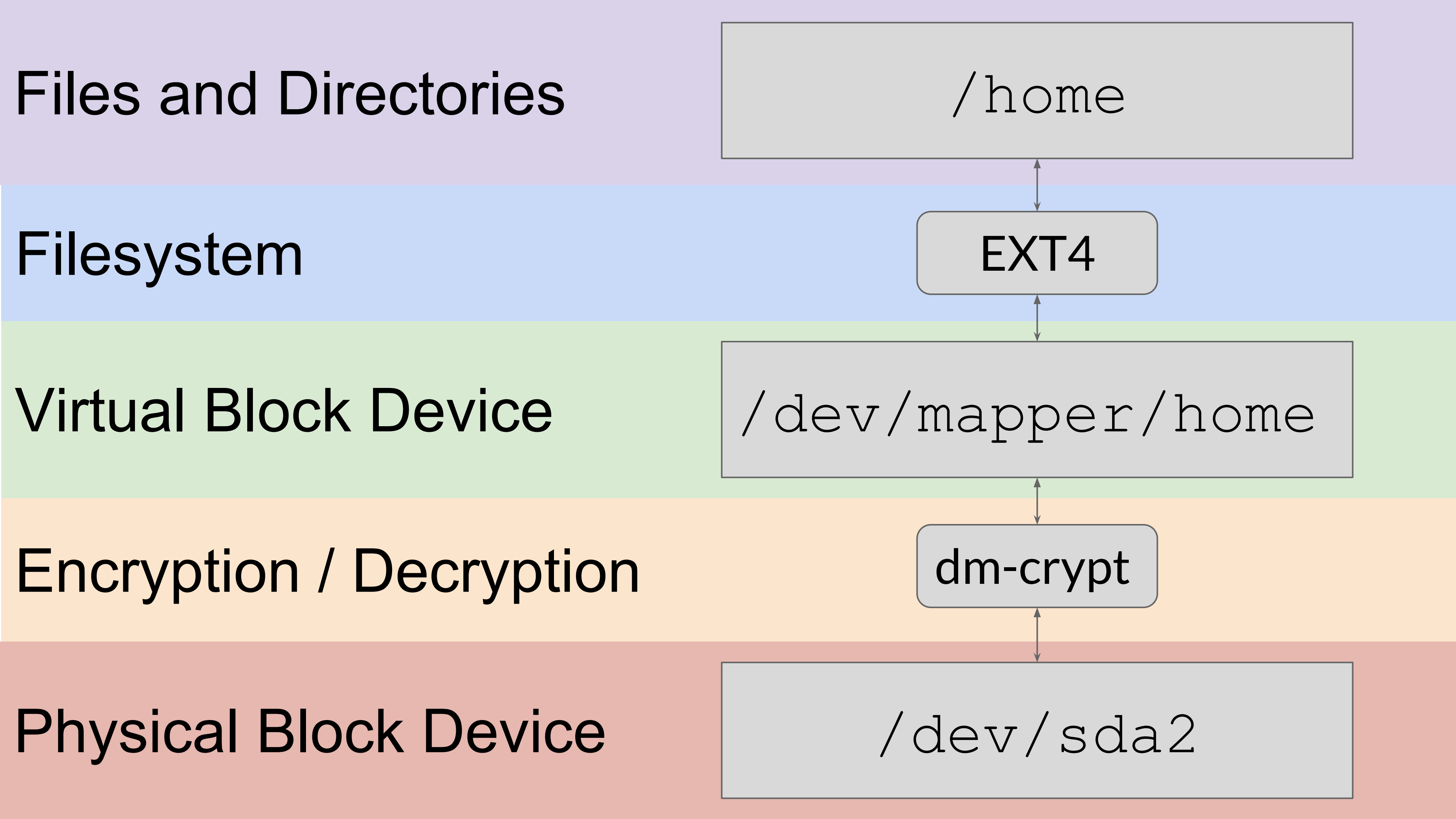
- Unlock (decrypt) data with a passphrase or a keyfile.
  - Used as the key OR used to unlock the actual key.
- The passphrase is a weak link.



https://commons.wikimedia.org/wiki/File%3ARack001.jpg

Disk Encryption for Linux

- dm-crypt - device mapper crypt
  - Provides transparent disk encryption.
  - Creates a new device in /dev/mapper.
  - Use like any other block device.
  - Manage with `cryptsetup`



Files and Directories `/home`

Filesystem EXT4

Virtual Block Device `/dev/mapper/home`

Encryption / Decryption dm-crypt

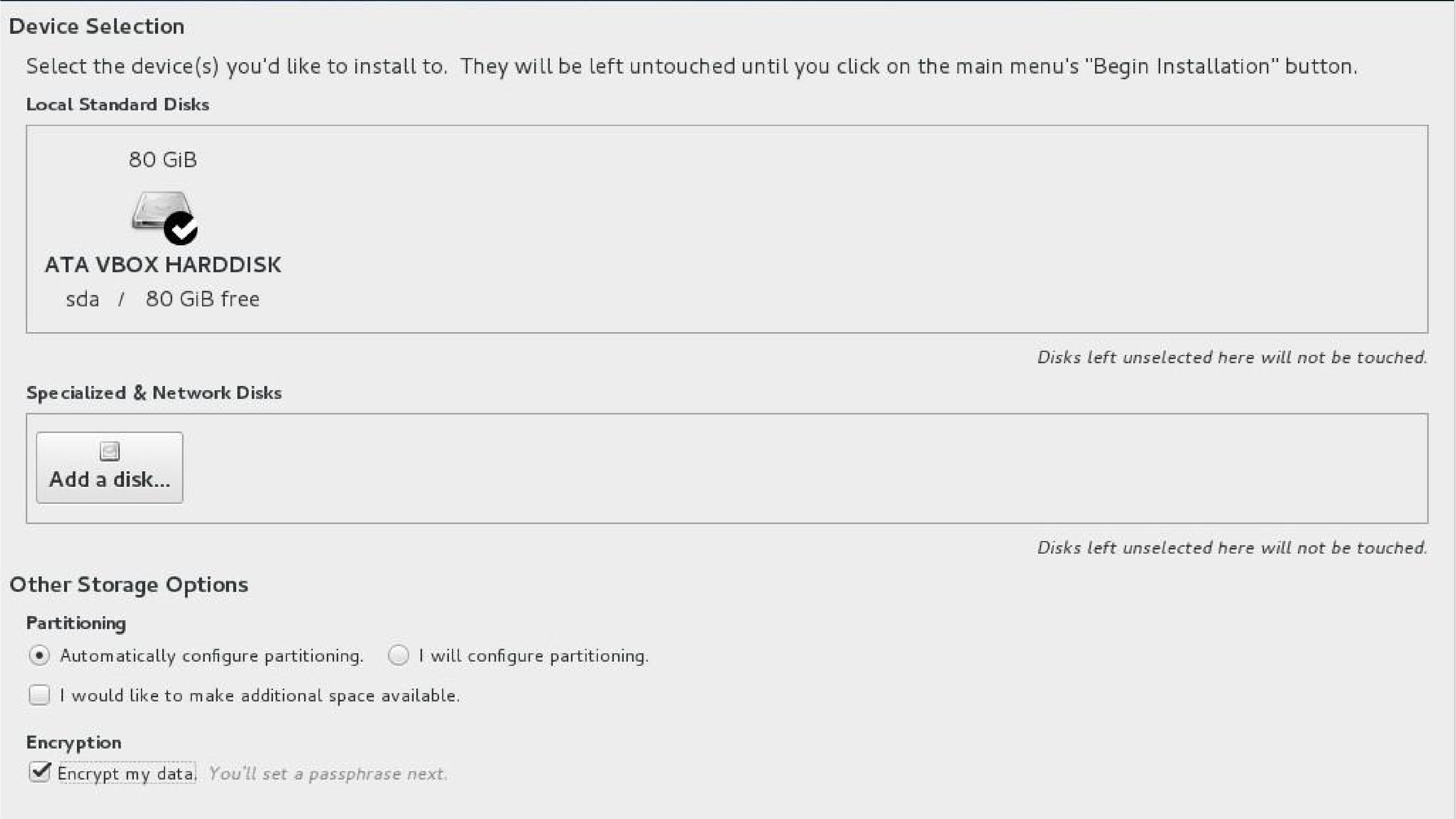
Physical Block Device `/dev/sda2`

LUKS

- Linux Unified Key Setup.
- Front-end for dm-crypt.
- Multiple passphrase support.
- Portable as LUKS stores setup information in the partition header.
- Great for removable media, too.

Encrypt During Install

- PRO: easy, with sane defaults.
- CON: you give up some control.



Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

80 GiB

ATA VBOX HARDDISK

sda / 80 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Other Storage Options

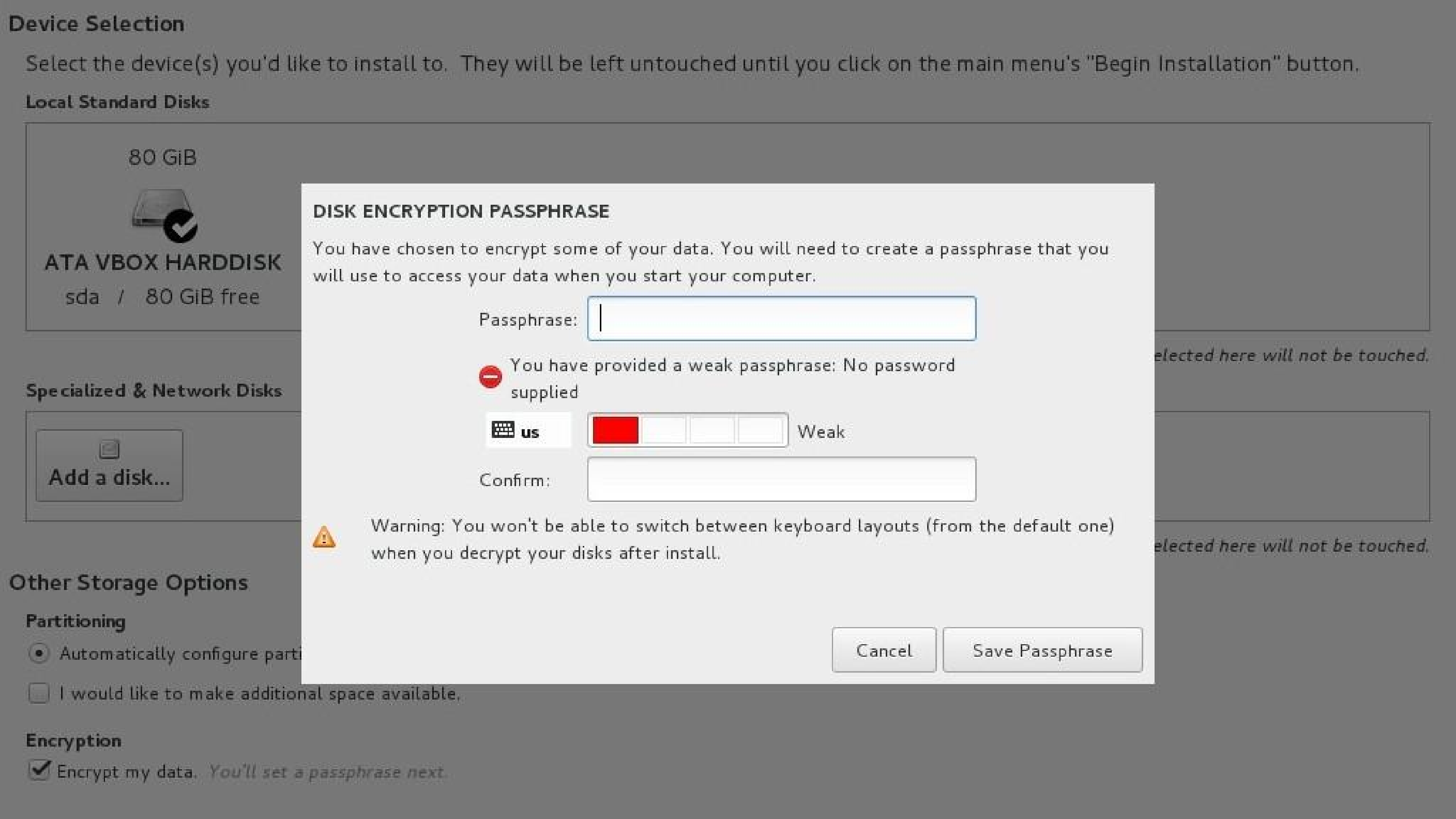
Partitioning

● Automatically configure partitioning. ○ I will configure partitioning.

□ I would like to make additional space available.

Encryption

☑ Encrypt my data. *You'll set a passphrase next.*



Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

80 GiB

ATA VBOX HARDDISK

sda / 80 GiB free

elected here will not be touched.

Specialized & Network Disks

elected here will not be touched.

Other Storage Options

Partitioning

● Automatically configure parti

□ I would like to make additional space available.

Encryption

☑ Encrypt my data. *You'll set a passphrase next.*

DISK ENCRYPTION PASSPHRASE

You have chosen to encrypt some of your data. You will need to create a passphrase that you will use to access your data when you start your computer.

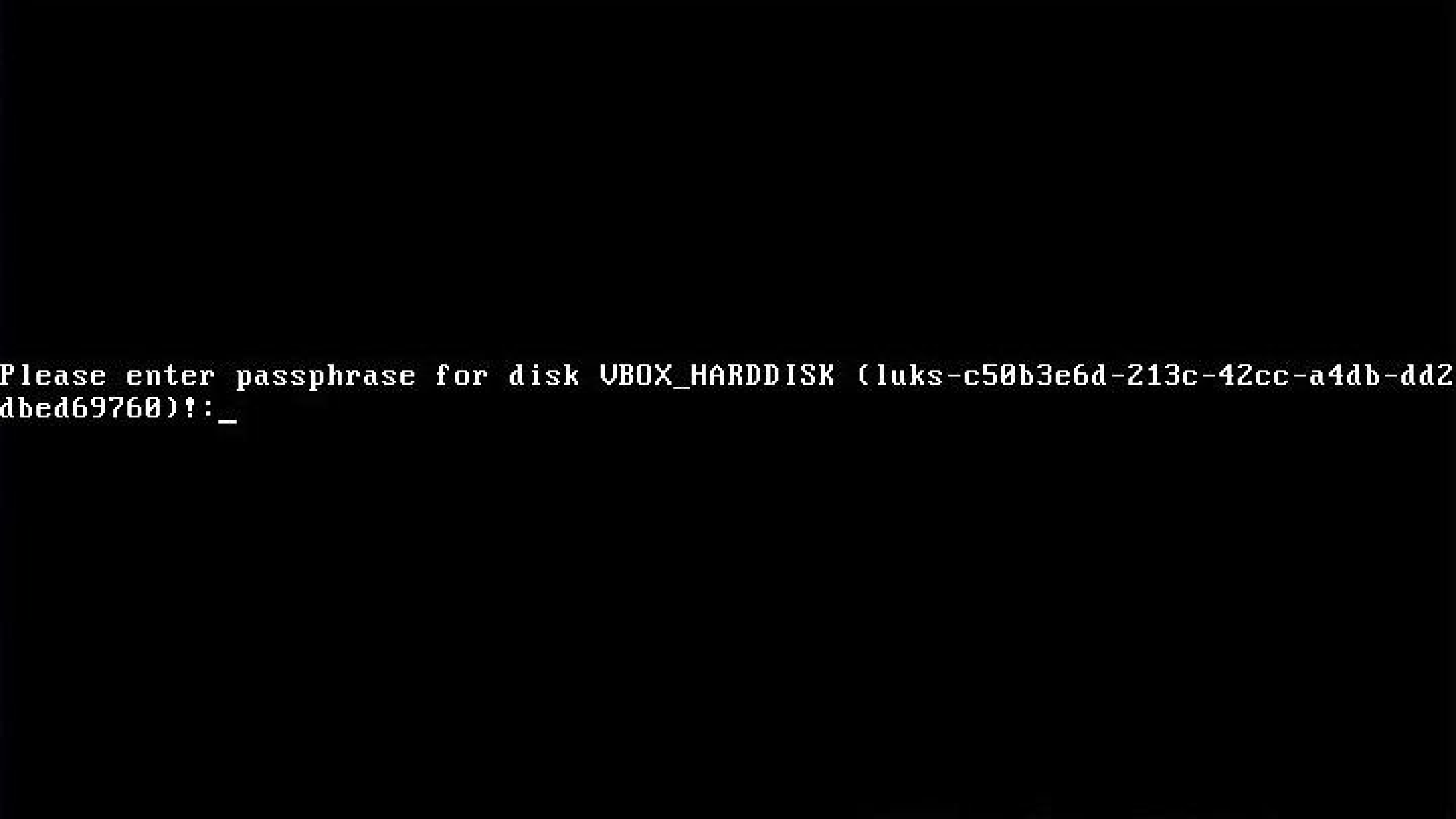
Passphrase:

You have provided a weak passphrase: No password supplied

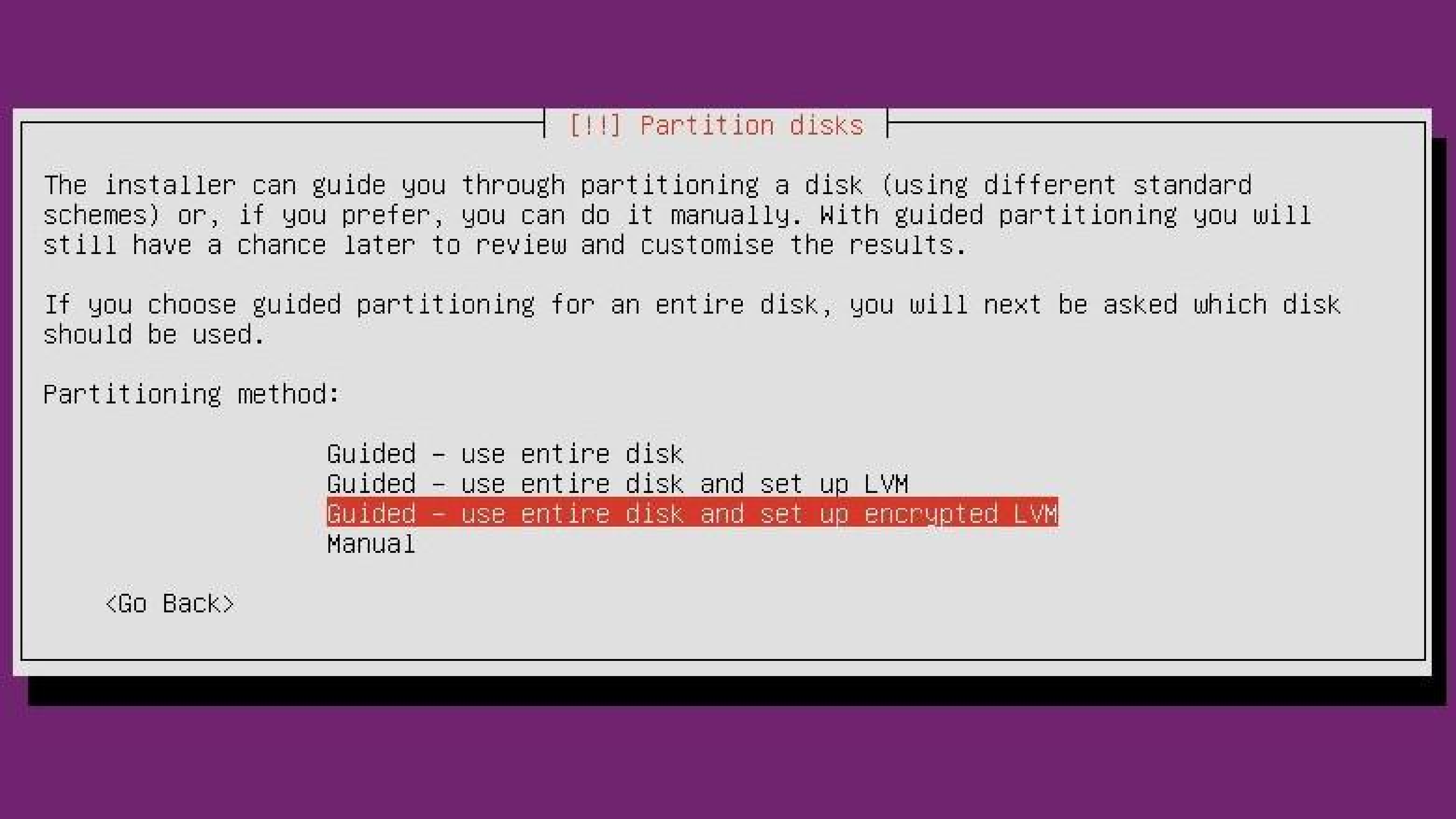
us 🟥 Weak

Confirm:

Warning: You won't be able to switch between keyboard layouts (from the default one) when you decrypt your disks after install.



```
Please enter passphrase for disk VBOX_HARDDISK (luks-c50b3e6d-213c-42cc-a4db-dd2
dbed69760)!:
```



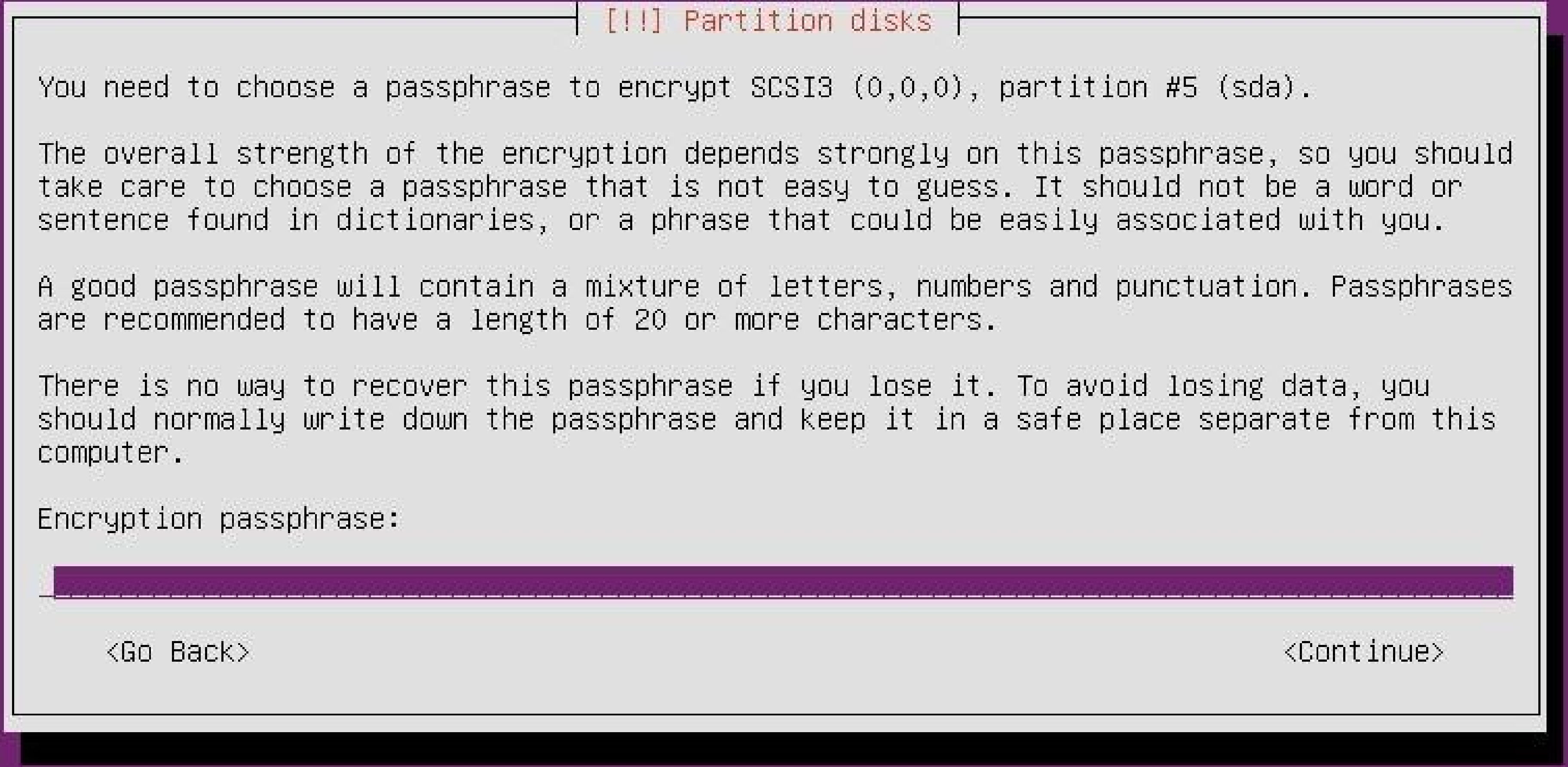
[!!] Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided – use entire disk
Guided – use entire disk and set up LVM
[✓ Guided – use entire disk and set up encrypted LVM]
Manual



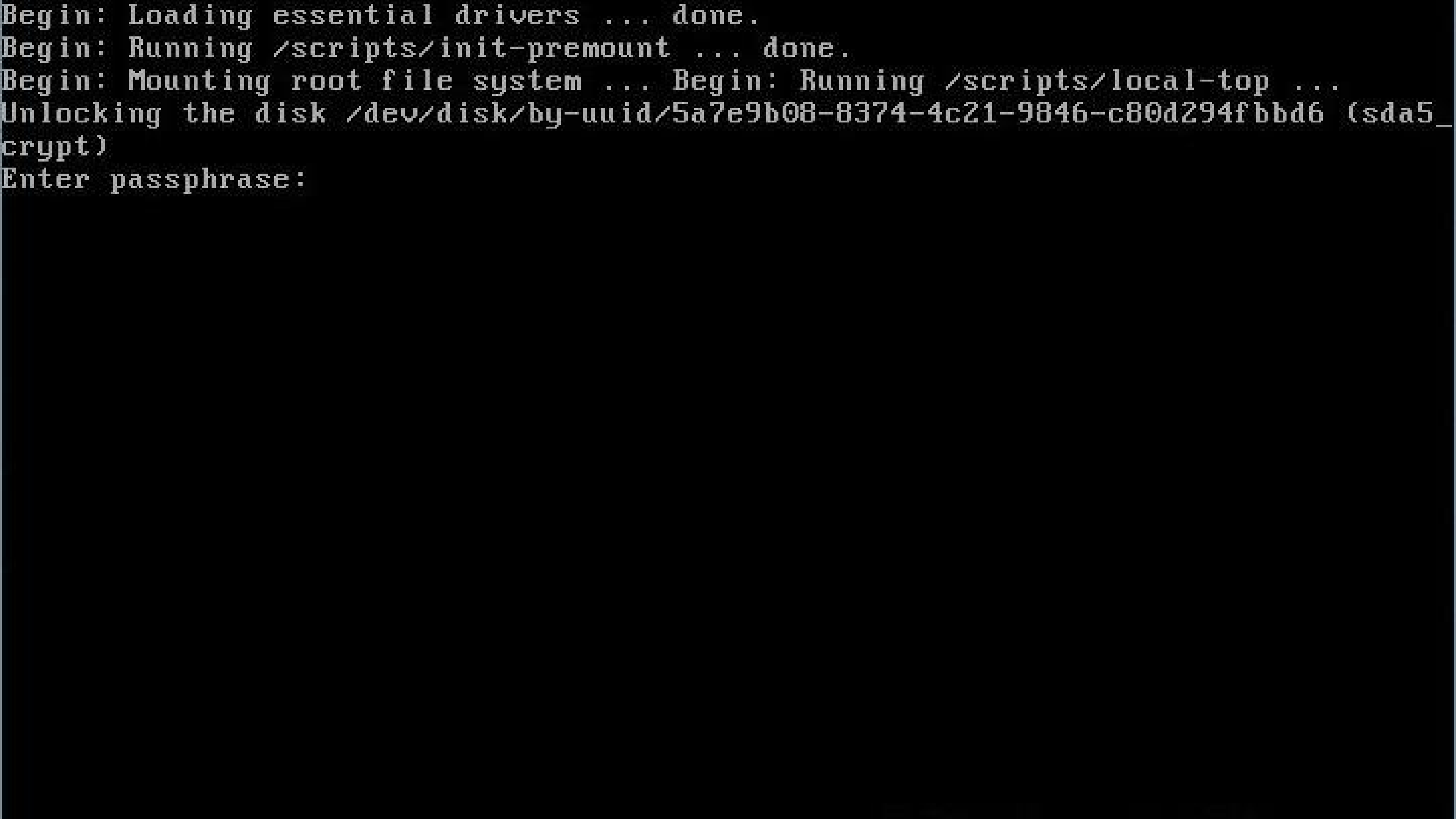
You need to choose a passphrase to encrypt SCSI3 (0,0,0), partition #5 (sda).

The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.

A good passphrase will contain a mixture of letters, numbers and punctuation. Passphrases are recommended to have a length of 20 or more characters.

There is no way to recover this passphrase if you lose it. To avoid losing data, you should normally write down the passphrase and keep it in a safe place separate from this computer.

Encryption passphrase:



```
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ...
Unlocking the disk /dev/disk/by-uuid/5a7e9b08-8374-4c21-9846-c80d294fbbd6 (sda5_
crypt)
Enter passphrase:
```

Setting up LUKS on a New Device

Setting up LUKS on a New Device

- Use this process for any block device presented to your system that you want to encrypt.
- Following this procedure **will remove all data** on the partition (device) that you are encrypting!

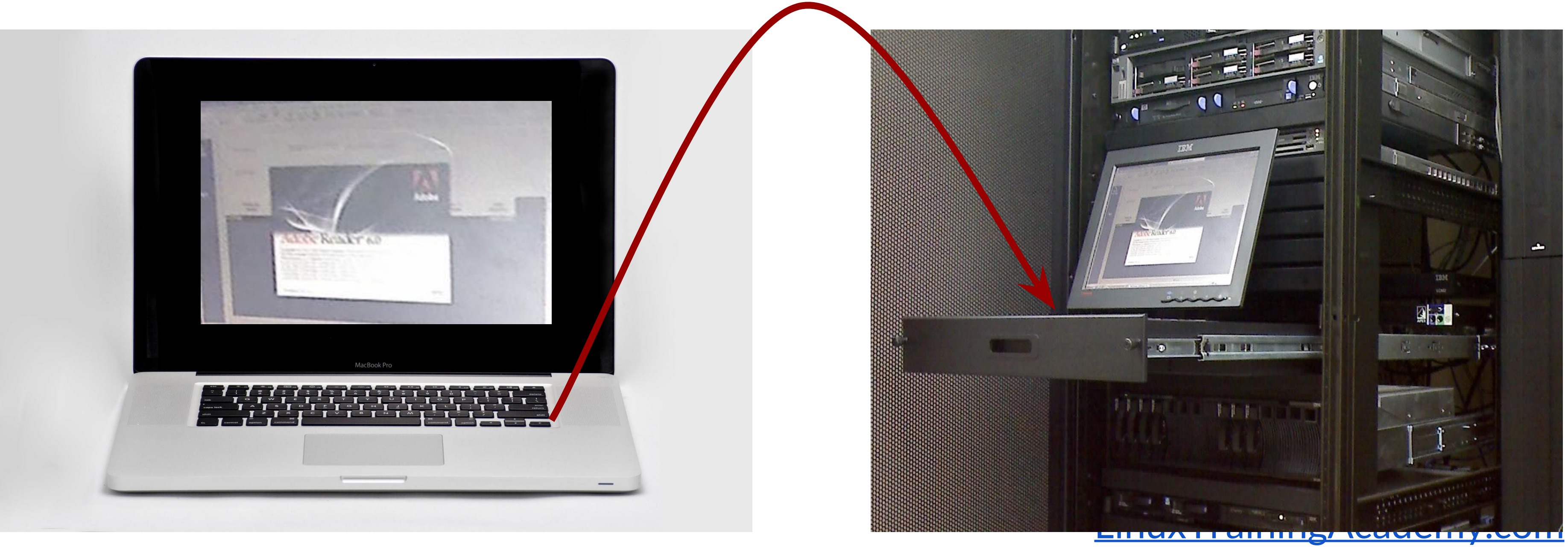
Converting a Device to LUKS

Converting a Device to LUKS

- Backup the data.
  - /home lives on /dev/sda3, for example.
- Wipe the device.
  - use shred or dd if=/dev/urandom of=/dev/sda3
- Setup LUKS.
  - cryptsetup luksFormat /dev/sda3
  - cryptsetup luksOpen /dev/sda3 home
  - mkfs -t ext4 /dev/mapper/home
  - mount /dev/mapper/home & restore from backup.

Disabling Ctrl+Alt+Del

- Remote consoles / network connected KVMs.



Disabling Ctrl+Alt+Del (Systemd)

```
systemctl mask ctrl-alt-del.target
systemctl daemon-reload
```

Section Summary

Summary

- Physical security threats.
- Physical security guidelines.
- Single user mode defenses.
- Kernel parameter protections.
- Disk encryption with LUKS.
- Disabling reboots from Ctrl+Alt+Del.