

Ubuntu Hacks

Virtual Virtual Devices: Encrypted RAID

Jonathan Oxer

OSCON
July 26th, 2006



Device Mapper

New feature in 2.6 kernel to layer arbitrary features on top of block devices

- Snapshotting
- Backups
- Redirection
- Encryption

Device Mapper Modules

Modules use the device-mapper framework to implement specific functionality:

- “dmraid” for software RAID
- “cryptsetup” for block device encryption

Alternative Systems

Cryptoloop and loop-AES are older approaches to filesystem encryption.

Cryptoloop has some disadvantages:

- Known plaintext attacks
- Watermark attacks

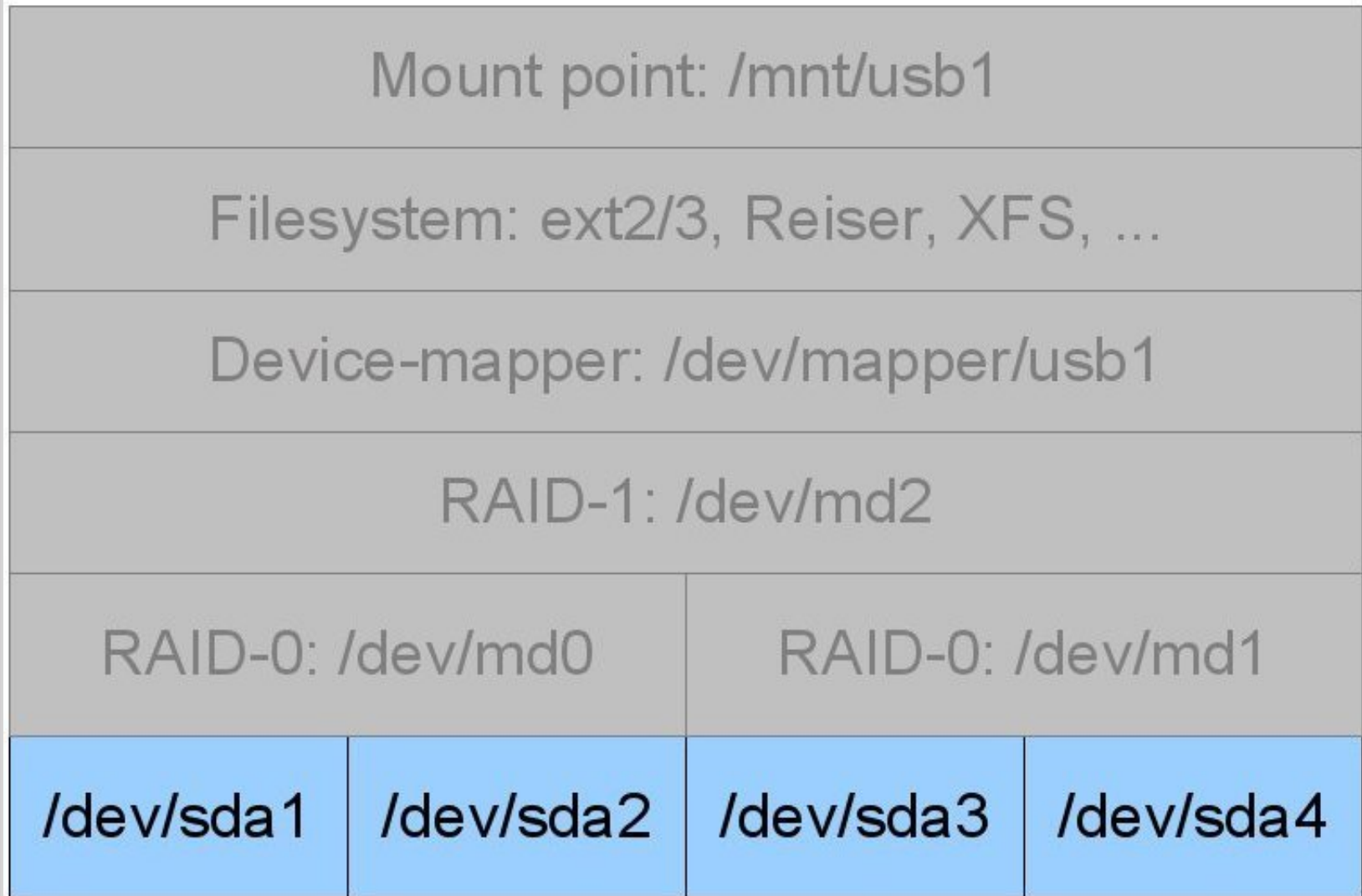
loop-AES is slower than dm-crypt and less flexible.

Caveats

Encrypted filesystems typically write faster than they read!

Absolutely do **not** forget your password ;-)

Layering Virtual Devices



Layering Virtual Devices

Mount point: /mnt/usb1

Filesystem: ext2/3, Reiser, XFS, ...

Device-mapper: /dev/mapper/usb1

RAID-1: /dev/md2

RAID-0: /dev/md0

RAID-0: /dev/md1

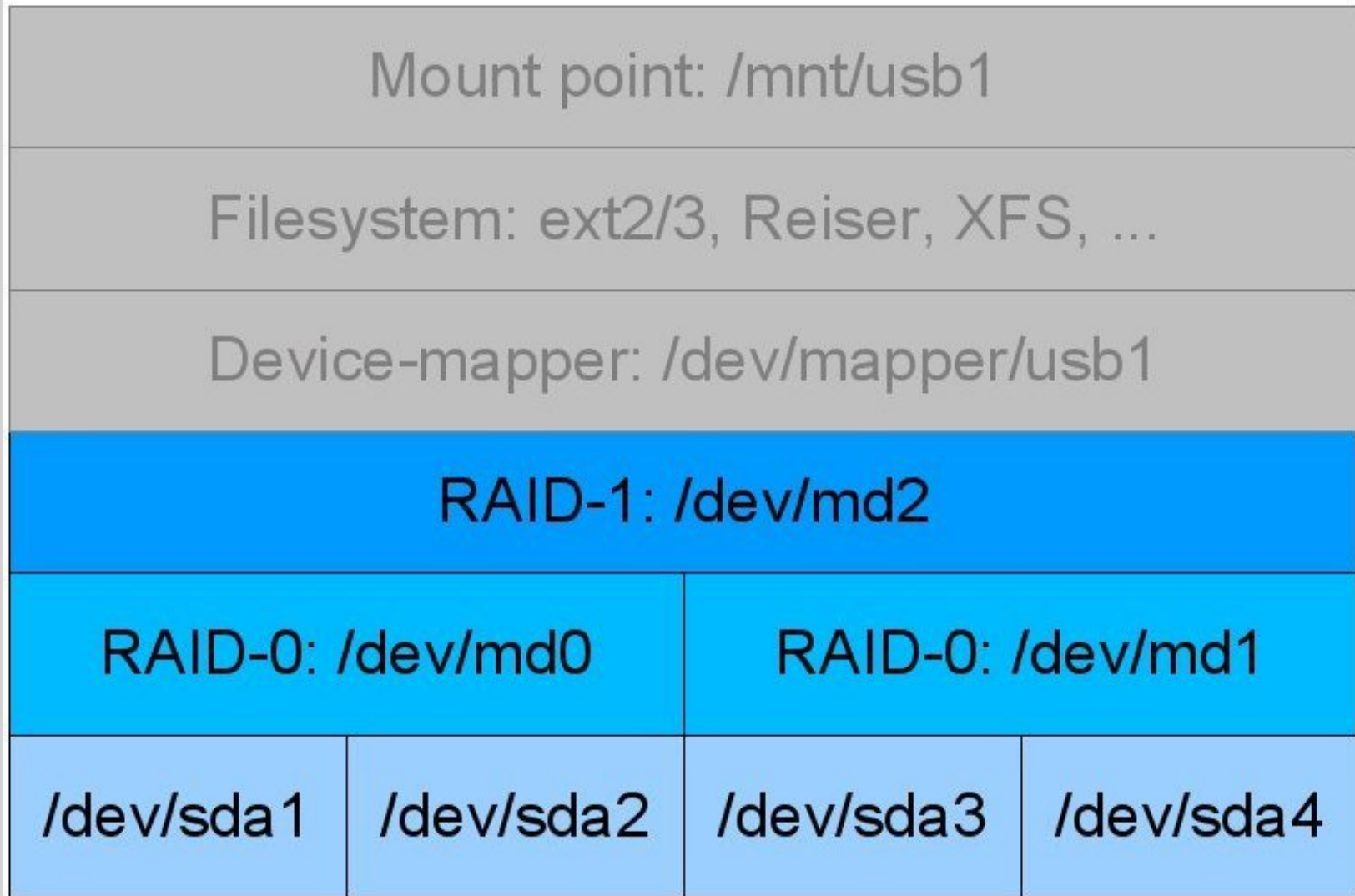
/dev/sda1

/dev/sda2

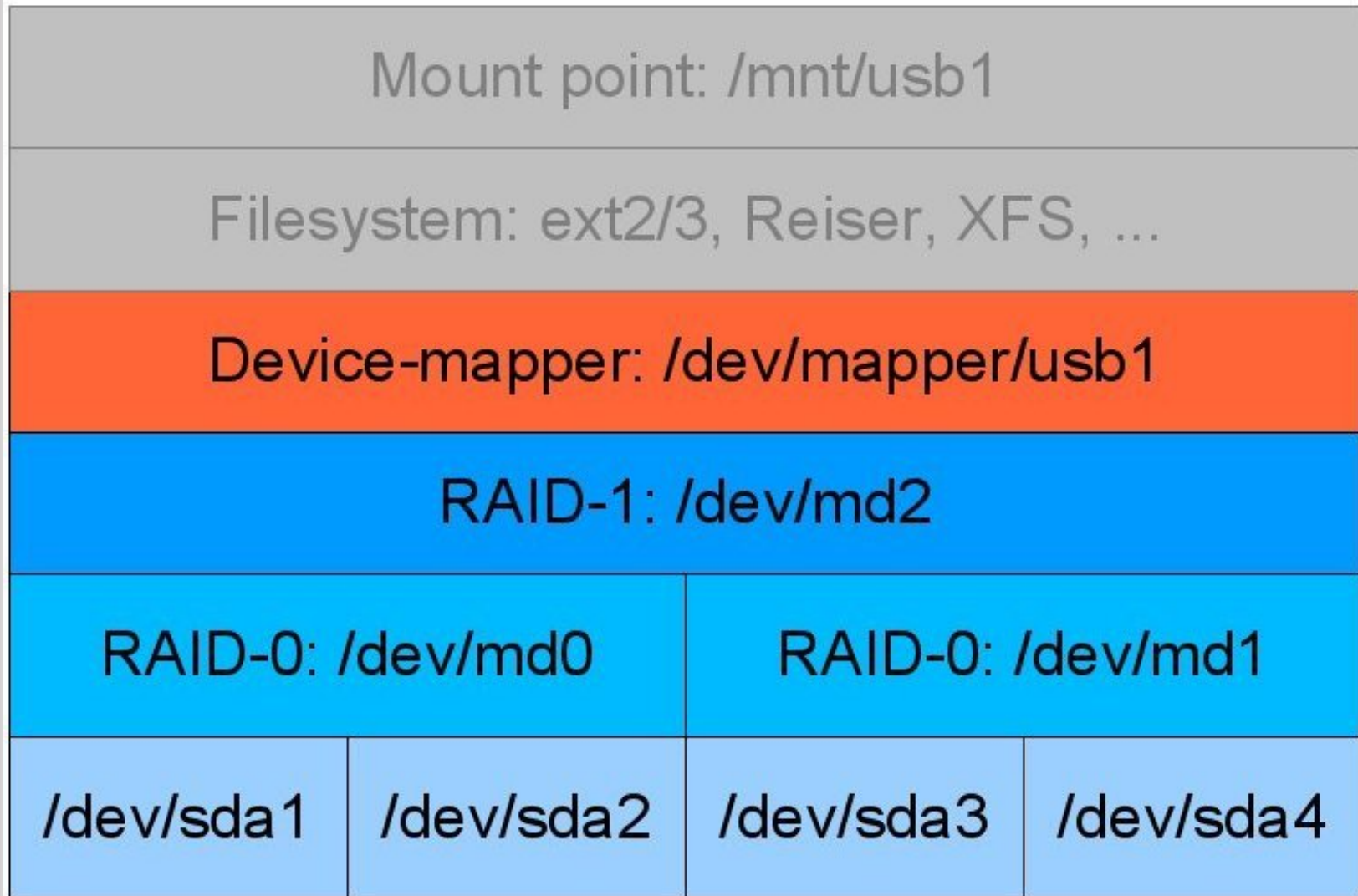
/dev/sda3

/dev/sda4

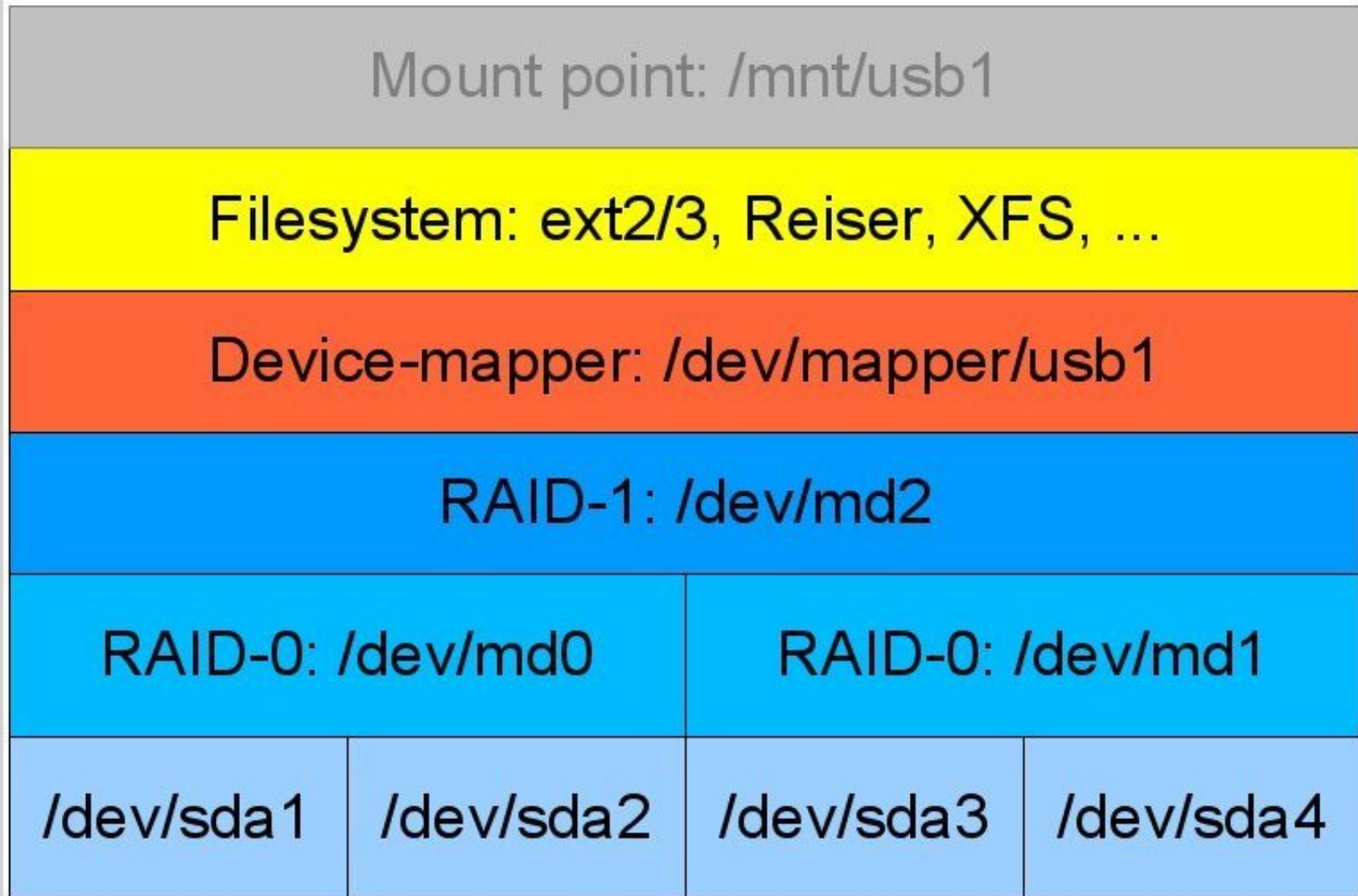
Layering Virtual Devices



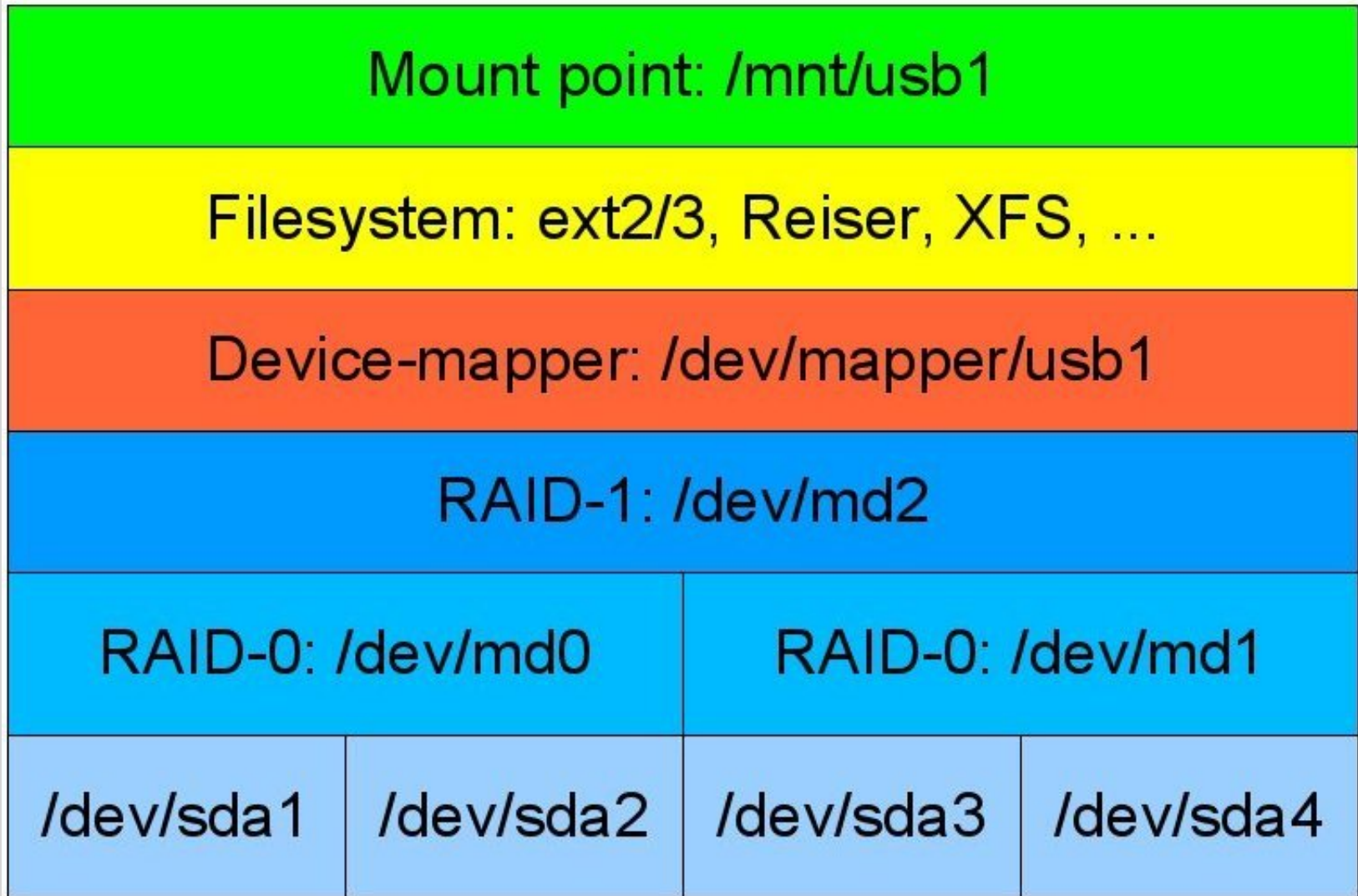
Layering Virtual Devices



Layering Virtual Devices



Layering Virtual Devices



Install Required Packages

Install device-mapper and cryptsetup packages:

```
sudo apt-get install cryptsetup
```

Create The Device Layers

- Create the pair of RAID-0 devices:

```
mdadm --create /dev/md0 --level=0 \  
  --raid-devices=2 /dev/sda1 /dev/sda2
```

```
mdadm --create /dev/md1 --level=0 \  
  --raid-devices=2 /dev/sda3 /dev/sda4
```

- Use those to create a RAID-1 device:

```
mdadm --create /dev/md2 --level=1 \  
  --raid-devices=2 /dev/md0 /dev/md1
```

- Create an encrypted virtual device:

```
cryptsetup create usb1 /dev/md2
```

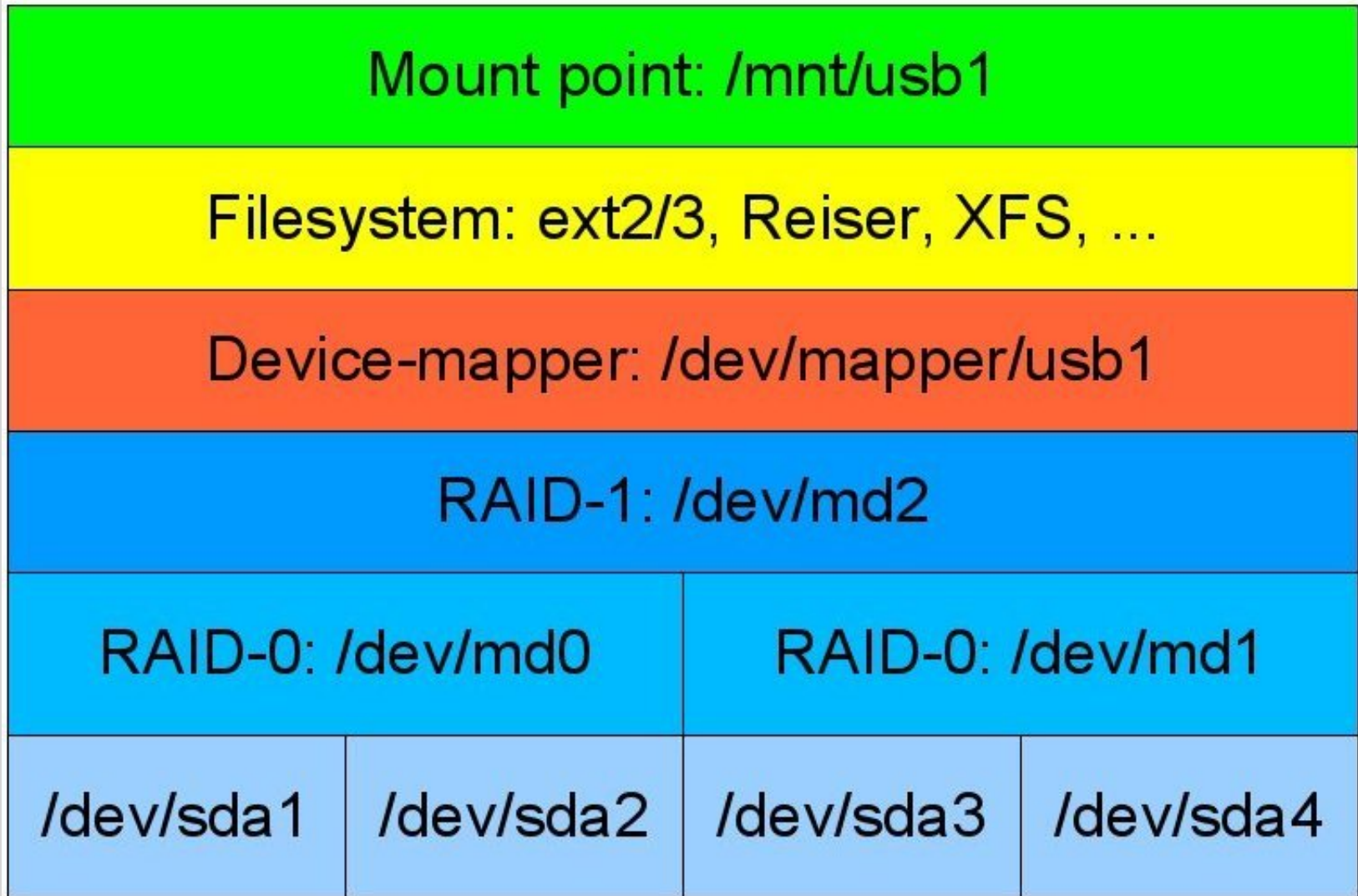
- Create a filesystem on the virtual device:

```
mkfs.ext2 /dev/mapper/usb1
```

- Finally, mount it:

```
mount /dev/mapper/usb1 /mnt/usb1
```

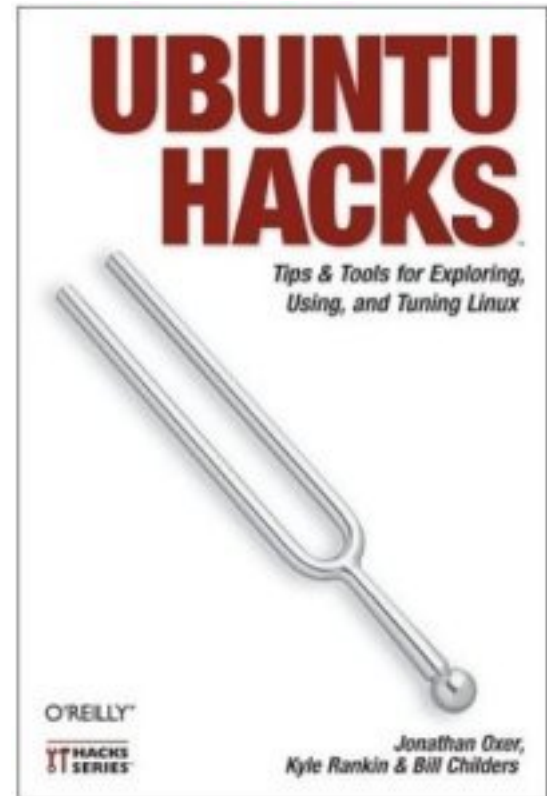
Layering Virtual Devices



More Information

These slides are online at:
jon.oxer.com.au/talks

Ubuntu Hacks available now:
www.ubuntuhacks.com



Thanks for listening!