Disk Encryption

An overview by Addison Amiri

What is Encryption and Why Do we Need it?

- Encryption hides things and prevents tampering
- Stop bad guys
- Offline attacks
- Inconveniences

Types of Encryption

Disk Encryption and File Encryption

Disk Encryption

- Protects all disk contents
- Everything is encrypted by default
- Password is asked once during mount
- One key is used
- Slowdown of whole system

File Encryption

- Only certain things are encrypted
- Mainly for specific files and folders
- Difficult to protect system files and folders
- Less overhead for operating system

Implementations of Disk Encryption

- True/Veracrypt
- DM-Crypt
- Luks/DM-Crypt

Deniable Encryption

- What is it?
- Why is it important?
- How is it implemented?

Considerations

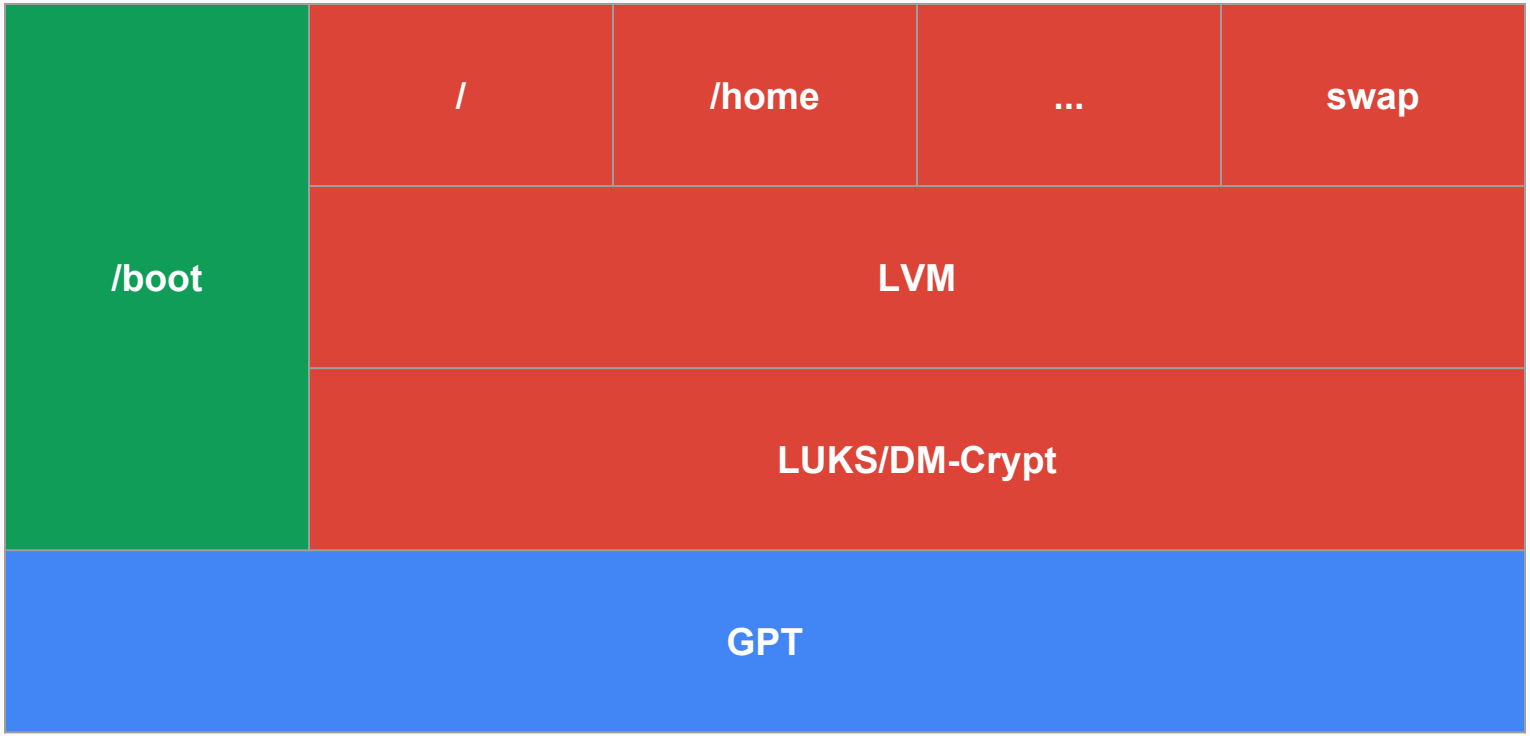
While setting up HDE it is important to consider the following things:

- Full Disk Encryption?
- Plausible Deniability?
- Swap?
- Data backups and drive wiping?
- Who are you trying to stop?
  - Multiple hardware access

Our Easy Encryption Setup

Overview

- LUKS/DM-Crypt
- LVM
- Partitions/Filesystems
  - Unencrypted /boot
  - Encrypted /
  - Encrypted swap
- Preformatting with /dev/urandom and trim on SSDs



Visualization of the Hard Drive after Encryption

Steps

0. dd if=/dev/urandom of=/dev/sda
1. Create two partitions
    a. or three for GPT+Grub
2. Format /boot
3. Cryptsetup
4. LVM
    a. Create Physical Volume (pvcreate)
    b. Create Volume Group (vgcreate)
    c. Create Logical Volume (lvcreate)
5. Format logical volumes
6. Set up boot*
    a. mkinitramfs
    b. kernel parameters

Demo

Closing Thoughts

Legal Issues

- Fifth Amendment
- In re Boucher (2009)
- Commonwealth v. Gelfgatt (January 2012)
- United States v. Doe (February 2012)
- Lavabit (2013)
- Outside the US

Questions?