Zymbit Hardware Security Module for Secure Internet of Things
Cybersecurity Malaysia 24-27 February 2020

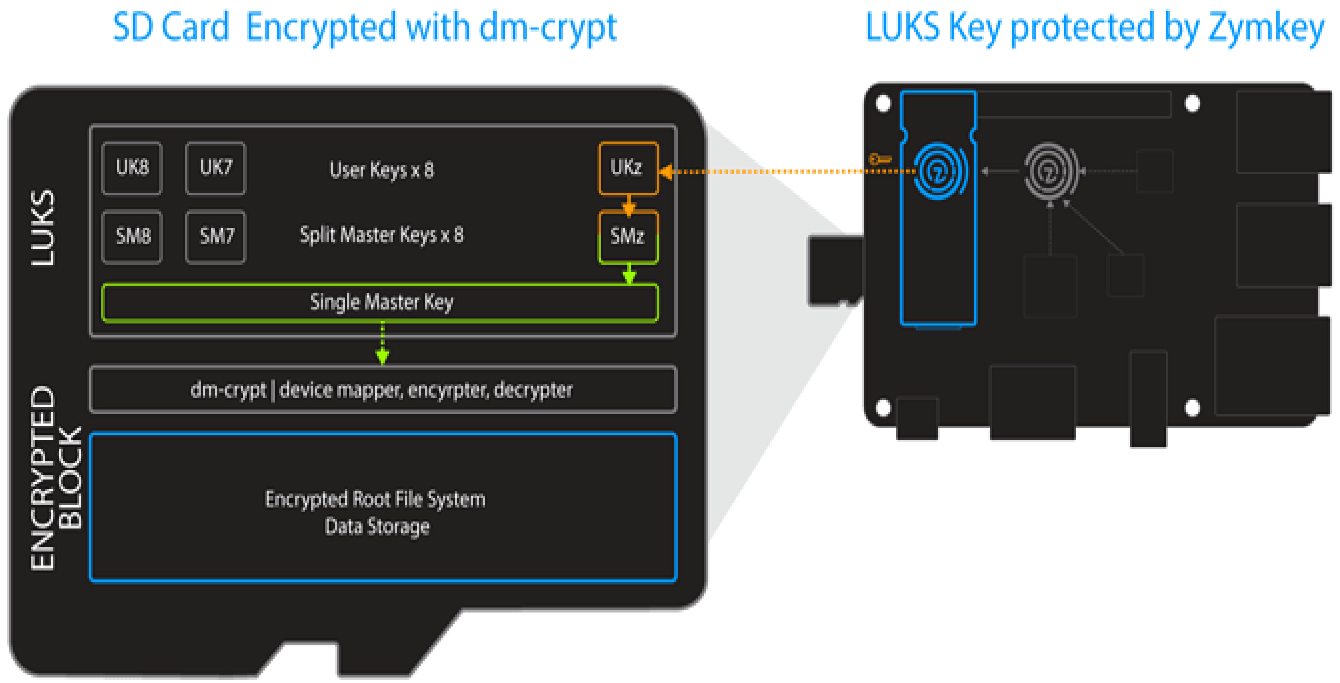
Module 3.1
Zymkey SD Card Encryption

CompuThings *Technology;

Module Target

- Understand how Zymkey linked with commonly used Linux file system encryption application
- Mount backup root file system at different machine.
- Prove root file system was encrypted by pulling out Zymkey from Raspberry Pi.

Zymkey SD Card Encryption


SD Card Encrypted with dm-crypt
LUKS Key protected by Zymkey
LUKS
UK8
UK7
User Keys x 8
UKz
SM8
SM7
Split Master Keys x 8
SMz
Single Master Key
dm-crypt | device mapper, encyrpter, decrypter
ENCRYPTED BLOCK
Encrypted Root File System
Data Storage

Run the Command First, Because It Takes Time

```
#cp /boot/cmdline.txt ~/boot_cmdline_bak.txt
```

```
#vim /boot/cmdline.txt
```

- Remove *quite* and save back, so we can see what happened in the background.

```
#wget https://s3.amazonaws.com/zk-sw-repo/mk_encr_sd_rfs.sh
```

- plug in your 32GB USB drive

- ensure your USB drive is *on /dev/sda.*

Run the Command First, Because It Takes Time...2

- Backup your data, because if encryption fails your data will lost.

```
#sudo bash mk_ecnr_sd_rfs.sh
```

and Wait.

Why Need to encrypt? Many Reason

- To keep wifi password and data safe
- Prevent data cloning
- In general Pi configuration, only two partition exist:
  - /boot on */dev/mmcblk0p1*
  - / on /dev/mmcblk0p2

What is LUKS

- Is the popular key management setup for dm-crypt, the de-facto standard for block device encryption with Linux.
- LUKS provides a robust and flexible mechanism for multiple users (and services) to interface to and access Linux’s ‘dm-crypt 45’ infrastructure.
- dm-crypt is a transparent disk encryption subsystem in Linux kernel versions 2.6 and later and is part of the device mapper infrastructure, and uses cryptographic routines from the kernel’s Crypto API.

Weaknesses of Single Master Key

- dm-crypt has a single Master Key that is used to encrypt / decrypt data in/out of the block.
- It would be necessary to change the Master Key frequently, and potentially share it with multiple users/services on a regular basis
- Every new iteration of Master Key would require the underlying data block to be re-encrypted every time.
- This is impractical

Hierarchical Key Management

- Users/services are given user keys that use to release master key.
- User Keys can be easily changed and revoked, without having to re-encrypt the underlying data block.
- The management of such a hirearchical key managers is the role of LUKS.
- Zymkey is use to lock a User Key, that is subsequently used to unlock the Master Key and provide access to the Root File System

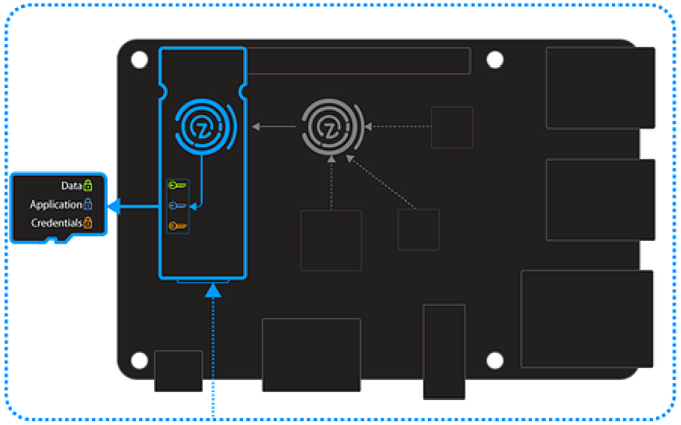
Securing LUKS User Key with Zymkey Security Module

- Zymkey provides a general “locking” service.
- When used with LUKS, the User Key is sent to the Zymkey to be locked (encrypted and signed) when the file system is created.
- Then the locked key is unlocked (signature verified and encrypted).
- The booting sequence as follows:
  - Kernel initialized initramfs
  - Initramfs presents the locked LUKS key to zymkey
  - Zymkey validates the signature and decrypt the key
  - Decrypted key is presented to LUKS and the root file system is then decrypted.

Zymkey Host Authentication

- Zymkey will create ID for a host system.
- This ID is used by zymkey to protect LUKS keys.

Device ID & Authentication with Zymkey



2 Options to do this

- Option 1: Encrypt current SD card and backup root file system to external drive
- Option 2: Migrate data to external drive and encrypt external drive.
- We take Option 1

Option 1

- We need to connect external usb drive.
- The script by default will look for rfs (root file system) and use */dev/sda* partition as external drive.
- It will take long time, take a break.
- When finish Rpi will reboot

After Reboot

- Rpi will normally reboot after the process. Congratulations.
- Power down Rpi
- Remove usb drive
- Mount usb drive to your laptop. Can you identify the partition type?
- Boot Rpi and examine your partition.
- Shutdown Rpi
- Remove Zymkey
- Can you boot your Linux?

Conclusion

This exercise is to show that we can use zymkey to encrypt our file system. This is very useful for real production grade system.