Full Disk Encryption

David Klaftenegger

Department of Information Technology
Uppsala University, Sweden

22. March 2019
this talk contains opinions
my opinions
not the university’s
nor do I claim to be an expert
... so expect some imprecision and errors
### What’s the problem?

### Why encrypt data?

- important to you
- protect in case of device loss?
- theft?
- police?
- nation state attackers?

**My choices**
- loss / theft
- broken device
- selling device
- singular access by evil maid

22 Mar 2019
What’s the problem?

Why encrypt data?

- important to you
What’s the problem?

Why encrypt data?

- important to you (that I can’t see it)
What’s the problem?

Why encrypt data?

- important to you (that I can’t see it)
- protect in case of
  - device loss?
  - theft?
  - police?
  - nation state attackers?
What’s the problem?

https://www.xkcd.com/538/
https://creativecommons.org/licenses/by-nc/2.5/
**What’s the problem?**

### Why encrypt data?
- important to you (that I can’t see it)
- protect in case of
  - device loss?
  - theft?
  - police?
  - nation state attackers?

### My choices
- loss / theft
- broken device
- selling device
- singular access by evil maid
Why Full Disk Encryption?

Shouldn’t I encrypt only important data?
Why Full Disk Encryption?

Shouldn’t I encrypt only important data
- lots of (personal) data on computer
- difficult to decide what is important
Why Full Disk Encryption?

Shouldn’t I encrypt only important data

- lots of (personal) data on computer
- difficult to decide what is important
- encrypt everything by default
- same security, less effort
Why Full Disk Encryption?

Shouldn’t I encrypt only important data
- lots of (personal) data on computer
- difficult to decide what is important
- encrypt everything by default
- same security, less effort

Shouldn’t I use better encryption for more important stuff?
Why Full Disk Encryption?

https://www.xkcd.com/538/
https://creativecommons.org/licenses/by-nc/2.5/
Which Software should I use?

There is a lot of alternatives
Which Software should I use?

There is a lot of alternatives

From wikipedia:

- Aloaha Crypt Disk
- ArchiCrypt Live
- BestCrypt
- BitArmor DataControl
- BitLocker
- Bloombase Keyparc
- Boxcryptor
- CGD
- CenterTools DriveLock
- Check Point Full Disk Encryption
- CipherShed
- CrossCrypt
- CryFS
- Cryhod
- Cryptainer
- Cryptic Disk
- CryptArchiver
- Cryptoloop
- Cryptomator
- CryptoPro Secure Disk Enterprise

Maybe not that important...
## Which Software should I use?

### There is a lot of alternatives

**From wikipedia:**
- Aloaha Crypt Disk
- ArchiCrypt Live
- BestCrypt
- BitArmor
- DataControl
- BitLocker
- Bloombase Keyparc
- Boxcryptor
- CGD
- CenterTools
- DriveLock
- Check Point Full Disk Encryption
- CipherShed
- CrossCrypt
- CryFS
- Cryhod
- Cryptainer
- Cryptic Disk
- CryptArchiver
- Cryptoloop
- Cryptomator
- CryptoPro Secure Disk Enterprise
- CryptoPro Secure Disk for BitLocker
- CryptSync
- Discryptor
- DiskCryptor
- DISK Protect
- Cryptsetup / Dmsetup
- Dm-crypt / LUKS
- DriveCrypt
- DriveSentry
- GoAnywhere 2
- E4M
- e-Capsule Private Safe
- eCryptfs
- EgoSecure HDD Encryption
- EncFS
- EncryptStick
- FileVault
- FileVault 2
- FinalCrypt
- FREE CompuSec
- FreeOTFE
- GBDE
- GELI
- GnuPG
- gocryptfs
- Knox
- KryptOS
- LibreCrypt
- Loop-AES
- McAfee Drive Encryption (SafeBoot)
- n-Crypt Pro
- PGPDisk
- Private Disk
- ProxyCrypt
- R-Crypto
- SafeGuard Easy
- SafeGuard Enterprise
- SafeGuard PrivateDisk
- SafeHouse Professional
- Scramdisk
- Scramdisk 4 Linux
- SecuBox
- SECUDE Secure Notebook
- SecureDoc
- Seqrite Encryption Manager
- Sentry 2020
- Softraid / RAID C
- SpyProof!
- Svnd / Vnconfig
- Symantec Endpoint Encryption
- Tcplay
- Trend Micro Endpoint Encryption (Mobile Armor)
- TrueCrypt
- USBCrypt
- VeraCrypt
- TrueCrypt License Version 3.0 (legacy code only)
- CyberSafe Top Secret
Which Software should I use?

There is a lot of alternatives

Some selection that you may want to look at:

- BitLocker
- Veracrypt
- LibreCrypt
- LUKS
- ZFS (native filesystem encryption)
Which Software should I use?

There is a lot of alternatives

Some selection that you may want to look at:

- BitLocker
- Veracrypt
- LibreCrypt
- LUKS
- ZFS (native filesystem encryption)

Maybe not that important...
Which Software should I use?

https://www.xkcd.com/538/
https://creativecommons.org/licenses/by-nc/2.5/
Features

General

- full encryption vs plaintext metadata
- open source
- plausible deniability ("hidden volume")
- protection against modification
- operating systems (Linux, Windows, Mac OS X, BSD, ...)
- multiple keys
Features

General (LUKS in bold)

- full encryption vs plaintext metadata
- open source
- plausible deniability ("hidden volume")
- protection against modification
- operating systems (Linux, Windows, Mac OS X, BSD, ...)
- multiple keys
Features

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <strong>full encryption</strong> vs plaintext metadata</td>
</tr>
<tr>
<td>- open source</td>
</tr>
<tr>
<td>- plausible deniability (&quot;hidden volume&quot;)</td>
</tr>
<tr>
<td>- protection against modification</td>
</tr>
<tr>
<td>- operating systems (<strong>Linux</strong>, Windows, Mac OS X, BSD, ...)</td>
</tr>
<tr>
<td>- multiple keys</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LUKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Linux Unified Key Setup</td>
</tr>
</tbody>
</table>
Features

https://www.xkcd.com/927/
https://creativecommons.org/licenses/by-nc/2.5/
Features

General

- full encryption vs plaintext metadata
- open source
- plausible deniability ("hidden volume")
- protection against modification
- operating systems (Linux, Windows, Mac OS X, BSD, ...)
- multiple keys

LUKS

- Linux Unified Key Setup
- random master key with eight key slots
- encrypts any block device (commonly: partition)
It’s really easy

Using LUKS

```bash
# cryptsetup -v --type luks --cipher aes-xts-plain64 --key-size 256 --hash sha256 --iter-time 2000 --use-urandom --verify --passphrase luksFormat /dev/mydevice
```
It’s really easy

# cryptsetup -v luksFormat /dev/mydevice
It’s really easy

Using LUKS

```bash
# cryptsetup -v luksFormat /dev/mydevice
WARNING!
This will overwrite data on /dev/mydevice irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase: correcthorsebatterystaple
Verify passphrase: correcthorsebatterystaple
Command successful.
```
It’s really easy

Using LUKS

```bash
# cryptsetup luksFormat /dev/mydevice
WARNING!
This will overwrite data on /dev/mydevice irreversibly.

Are you sure? (Type uppercase yes): YES
Enter passphrase: correcthorsebatterystaple
Verify passphrase: correcthorsebatterystaple
```
It’s really easy

Using LUKS (optional step)

```
# cryptsetup luksOpen /dev/mydevice crypto
Enter passphrase for /dev/mydevice:
   correcthorsebatterystaple

# dd if=/dev/zero of=/dev/mapper/crypto
# cryptsetup luksClose /dev/mapper/crypto
# cryptsetup lusKFormat device
WARNING!

This will overwrite data on /dev/mydevice irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase: correcthorsebatterystaple
Verify passphrase: correcthorsebatterystaple
```
It’s really easy

Using LUKS

```bash
# cryptsetup luksOpen /dev/mydevice crypto
Enter passphrase for /dev/mydevice: correcthorsebatterystaple

# mkfs.ext4 /dev/mapper/crypto
# mount /dev/mapper/crypto /home
```
It’s really easy

Using LUKS

```
# cryptsetup luksOpen /dev/mydevice crypto
Enter passphrase for /dev/mydevice: correcthorsebatterystaple

# mkfs.ext4 /dev/mapper/crypto
# mount /dev/mapper/crypto /home
```