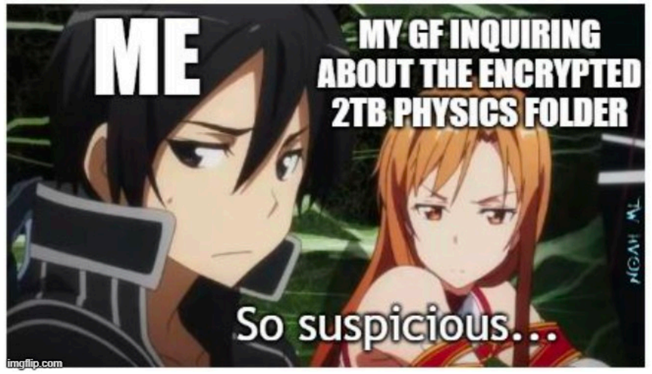
Disk Encryption

Applied Cryptography

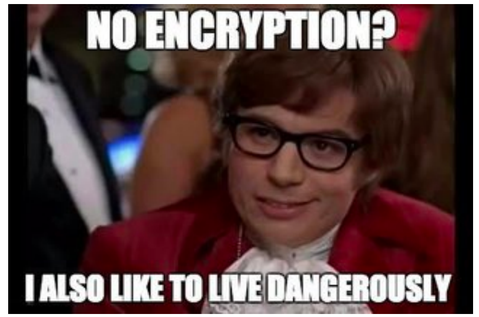
Encrypting Data At Rest



https://imgflip.com/i/45j7ie

- Several tools have been looked at this semester that can encrypt files
- Lots of office automation applications and even simple text editors have the ability to encrypt their files
- If you only need to protect a small number of specific files, these tools will likely provide everything required
- If you have a larger number of files, or your need for protection is not specific to any particular files, whole disk encryption is an option
- Encrypting data in files or file containers such as filesystems or drives is always done with symmetric encryption

Encrypted Drive Concepts



https://www.kinetix.com/blog/what-is-data-encryption

- Encrypting the full drive protects against theft, or unauthorized loaning/borrowing although the latter also requires policy and user education to be in place
- Encrypted drives do not require erasure when reselling, although it is still a good idea for HDDs
- Encrypting drives mitigates exposures related to seizure of equipment
- Encrypting the boot drive prevents unauthorized boot
- Whole drive encryption provides some security against forensic techniques as well, but also makes it considerably more difficult to regain access when the key is lost (practically impossible with modern encryption)

Encrypted Drive Implementations

- Disk storage can be encrypted in software by filesystem or block device driver code, or by using embedded drive hardware
- Filesystem or block device driver code for encryption can encrypt data regardless of where it is stored, on physical devices or in logical containers (files), although they can have problems when used with file shares
- Drives that have encryption hardware built in are called SEDs
- SEDs come in various flavours and capabilities that affect their effectiveness
  - ATA standard has both a master and user key
  - TCG's Opal standard provides considerably more flexibility in managing encrypted spaces on SEDs and is the only one you should consider using

SED

- Self-encrypting drive

TCG

- Trusted Computing Group

SED Key Management

https://stephenroughley.com/category/security/

- The problem of securing data at rest is significantly different from securing data in flight and so is the key management
- The authentication of both the storage device and the accessor is based solely on the keys
- Disk encryption is always full drive, symmetric only and the MEK/DEK is set at the factory and does not change in normal operation, crypto erase means delete the MEK/DEK
- Key wrapping, aka tiered encryption, aka envelope encryption, is used to have a MEK/DEK which is secured by a KEK
- TCG's Opal standard allows for multiple KEKs that apply to storage space ranges on drives

MEK

- Media Encryption Key

DEK

- Data Encryption Key

KEK

- Key Encryption Key

Windows Filesystem Encryption

- Microsoft provides Bitlocker (eDrive) with Windows, the latest in a line of disk and file encryption tools
- Bitlocker will automatically use Opal SED if it is available without telling you it did that
- Many 3rd party programs are available to encrypt part or all of a filesystem
- Bitlocker is managed from the Windows setting gui tools

MacOS Filesystem Encryption

- Apple's disk encryption tool called FileVault has been part of MacOS since 2003
- In addition to providing full drive encryption, it integrates with their Find My Mac cloud service to allow remote drive erasure in the case of stolen hardware
- FileVault is enabled and disabled in the system settings gui tool
- Many UNIX encryption tools run on MacOS, providing a similar command line encryption capability to Linux

Linux Filesystem Encryption

- ext4 filesystems and a few others can be encrypted transparently on a per-directory tree basis using the fscrypt library
- A single master key is used per tree, with distinct derived keys for every file
- File names and data are encrypted, metadata is not
- Different users can use different keys to encrypt their own distinct tree(s) in the same filesystem
- dm-crypt is a block-level device driver to encrypt storage devices which can then hold any kind of filesystem, and is often implemented with the Linux Unified Key Setup (LUKS) using the cryptsetup tool
- eCryptfs and EncFS are stackable filesystem encryption tools
- The ArchLinux wiki has an excellent chart showing data at rest encryption tools for Linux

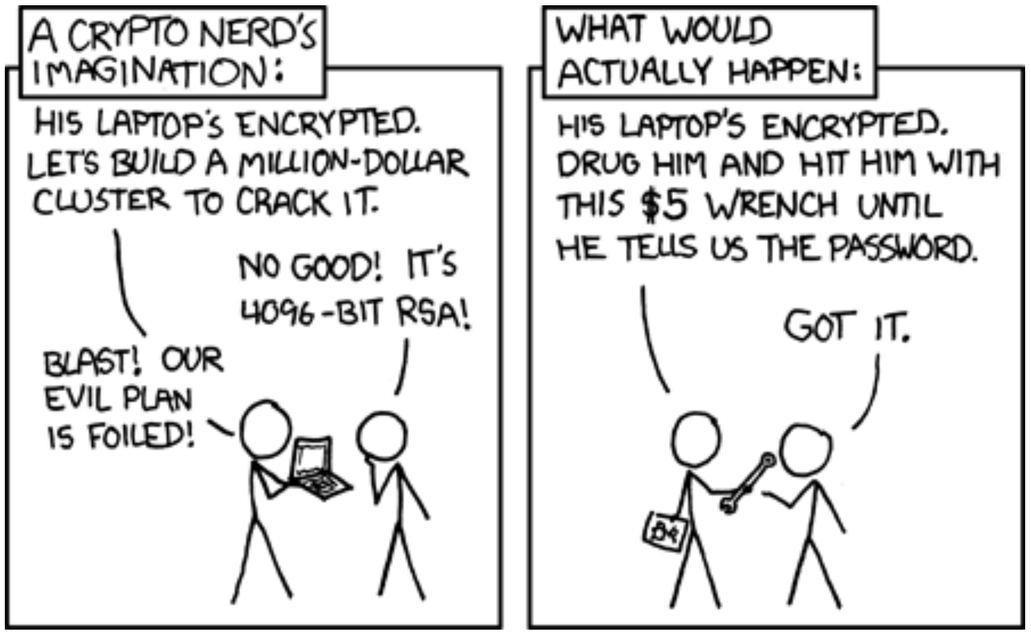
Veracrypt

- VeraCrypt is a container encryption tool that allows you to create filesystems in encrypted regular files that are stored in an unencrypted filesystem
- These are similar to ISO files used for software distribution
- VeraCrypt is the replacement for TrueCrypt which ran into legal troubles as well as suffering from discovered vulnerabilities
- VeraCrypt is open source and cross-platform
- Since a VeraCrypt container has a filesystem inside of it, it is very portable
- Container-based encryption tools like VeraCrypt create plausible deniability (although it can be exposed under the right circumstances)

Tomb

- tomb is a cli tool to create encrypted containers for files
- Tomb is OSS and is a shell script that uses the building blocks already discussed for encryption on the command line
- Like VeraCrypt/TrueCrypt/etc., it creates an encrypted filesystem that can be mounted and unmounted

Disk Encryption
Effectiveness



https://imgs.xkcd.com/comics/security.png

- SEDs provide a number of features that enhance security but also depend on the manufacturer to not take shortcuts with a black box solution
- FS encryption tools allow for endless variation in implementation and key rotation schemes but require the implementer to be knowledgeable and up to date
- No system is foolproof