**Intro to Disk Encryption**

**Encryption is a technique where data is converted into unreadable format so that only authorised people can read it**

A disk can be internal, external, USB, SD, DVD, CD, loopback device (like ISO), most storage devices that are readable as a file system

Software based disk encryption

* LUKS
* VeraCrypt
* TrueCrypt
* CipherShed
* BestCrypt
* FileVault2
* BitLocker

Many SSDs come with hardware encryption called self-encrypting drives (SED)

Whole disk encryption is when the whole OS and user data is encrypted

* Name suggests that everything is encrypted which isn’t true, especially with software-based encryption
* The boot and swap partitions can be unencrypted even with FDE, as well as the master boot record

Some hardware-based SED can provide real FDE

Partition/container encryption

* Encrypts just the selected user data within the partition

**What does disk encryption protect you from?**

* When your adversary can gain physical access to your device
  + Only readable when the OS is running and when they key has been entered
    - When lost or stolen
    - When seized
    - Left unattended around untrusted people
    - Sent for hardware repair
    - Sent through postal service
    - When crossing borders
    - When you want do securely discard it
* Can also help maintain integrity
  + Helps mitigate tampering
  + Preventing installation of rootkits, key loggers and general malware which can decrypt your keys
  + Due to encryption, bytes (malware) can’t just be added onto the disk, if they are, the disk won’t operate properly before removal
* Physical access to your device
  + Password can easily be bypassed
  + Filesystem cannot be explored when fully encrypted

**What does encryption NOT protect you from?**

* Anything that isn’t physical
  + Traffic
  + SSL stripping
  + Browser attacks
* No protection when system is on as key is kept in memory
* Once drive is decrypted, the key is in memory
  + Anyone who can get access to the memory can get to the key and decrypt your device
* Cold boot attack – the key can remain in memory for a short time after the device has been shut down
* No protection from coercion in countries that force you to give up encryption keys
* Little protection from an adversary who’s already tampered with your device
* When files are backed up elsewhere, they must also be encrypted or they have no protection