**File Encryption, Key Disclosure and Obfuscation**

**File encryption tools**

**PeaZip (Windows, Linux, OpenBSD)**

Open-Source file compression archiver that also has encryption

* 2FA
* Password
* AES-256 etc.

**Keka (MAC)**

**Key Disclosure**

Many countries require you to give up your keys by law

Mitigations can include

* Steganography
  + Adversary might not even know the data exists in the file they’re looking at
* Hidden OS
* Hidden Containers
* Encrypted partitions with no encryption signature
  + **Plausible deniability**
  + **Data is encrypted in a way that prevents an adversary from being able to prove that the data they are after even exists**
    - Plain dm-crypt – appears as simply an unformatted partition
* Hidden containers/volumes/Oss
  + One password can be used to decrypt a benign container containing non-critical data
  + And another password can be used on the same volume to decrypt a hidden volume with sensitive data on
  + BestCrypt can have many hidden containers
  + VeraCrypt can only have 1 hidden volume
    - Also don’t contain any encryption signatures, appearing as an unformatted partition
    - The excuse of having this random partition is that you have recently wiped or securely erased the content of it
  + Mustn’t contain any meta-information leaks
    - Items in the registry pointing to things that aren’t there
    - A hidden OS that when opened, hasn’t been updated or accessed in months, looks suspicious

**Some reasons why you might not want to use plausible deniability**

* If your adversary doesn’t act justly, then this may not be the best option
* If you are under oath, then lying could be worse than refusing the decryption information

**Reasons you may want to use plausible deniability**

* Could buy you time to work out your next move
* If you are in a just society, it could enable you to provide decryption information (to a decoy) whilst also maintaining your security and privacy

**Nesting Crypto Systems**

Software WDE (Foundation)

SED with password to give you access to drive in general

* Extra layer of protection with no detriment to performance

Encrypt system partition (OS)

Separately encrypt different volumes with data sets in them

* Each volume will only be opened when necessary as they are only mounted when used
  + Normal OS = Key 1
  + Top secret data = Key 2
  + Secret data = Key 3
  + Confidential data = Key 4
  + Non-sensitive data = Key 5
* Use different technologies to encrypt each layer
  + Each volume and system partition will have different passwords, different key files, 2FA etc.
  + Mitigate against bootloader attacks
  + Keep encryption keys of unmounted volumes out of memory

Hidden OS/ containers/ Volumes

* 2FA

Encrypt file archives

Encrypted VMS using hypervisor

* Can do WDE within VM guest
* Can put encrypted container within VM
* Nest VMs within each other and encrypt those

Hardware

* Encrypted USBs, SD with hardware encryption
  + Could even use software encryption as well
* Some have self-destruction
* Steganography to hide encrypted file on USB