**Defence Against Disk Encryption Attacks**

**Set-alerts for tampering**

* Place a barely viewable item on the device and if it moves then you will know
* Clear nail varnish under the object
  + Can boot up a hidden OS as a decoy partition if it has been tampered with, for plausible deniability etc

Power down the Device when unattended

Disable DMA supporting ports

* Done in the BIOS which is superior to doing it in the OS

Use WDE/FDE

Pre-boot Authentication with WDE

* Multi-Factor authentication
* Encrypt bootloader or place it on external USB so that it has to be inserted

Avoid SSDs

* As they use the trim cmd and wear levering

Don’t put sensitive data onto a drove until its encrypted

* Some crypto systems can leave traces of the clear text after it’s been encrypted
* So, encryption must be done first, then put data on it

Can use tools like TRESOR to mitigate Cold Boot Attacks

* Stores encryption keys on registry logs instead of RAM
* Tape up the device
* Superglue the memory
* Superglue the screw heads
* All of which will delay the memory being removed, the longer it takes, the more degradation
* No attacks yet on DDR4 memory?

Enable power-on self-test in the BIOS

* A self-check that’ll overwrite the RAM and mitigate a cold boot attack

Set a BIOS boot password

Disable the various ways that the memory can be dumped to disk

* Putting the system into hibernation or sleep

Swap file or virtual memory file can hold sensitive information in partition encryption