**Physical & Virtual Security Domains**

**It can be hard to find an OS that works for high security, high privacy, ease of use and speed**

* So, it may be necessary to **use multiple Operating Systems or physical machines**
* **One for security/privacy and one for general use** (low security domain)
* **Or use Hypervisors for your high security domain** e.g., Virtual Machines

The level of security needed to maintain privacy is not suitable for day-to-day use of the internet

**Physical Security Domains**

* A different device configured for security

Examples where this is necessary

* If you need to enter a country that forces you to give up your username and password for your laptop, just bring your daily
* A threat agent that could visit your location
  + Could hide the secure laptop and be okay with compromising your standard laptop
* When connecting to local networks
* Remember to buy physical machines anonymously because they each have a unique MAC address (Media Access Control address)

**Virtual Security Domains**

* Dual booting
* Platform virtualisation software/ hypervisors
* Hidden operating systems e.g., VeriCrypt, TrueCrypt
* Non-persistent OS e.g., Tails
* Bootable USBs
* OS’s designed for virtual separation like QubesOS