**QubesOS**

**Based on Xen hypervisor**

**Uses virtualisation to ensure compartmentalisation and isolation**

* This reduces the interfaces between security domains
* But still allows security domains to exist and communicate

**Kernel Design**

**TCB –** Trusted Computing Base

* All hardware, firmware and software that are critical to a systems security
* If compromises happen within the TCB, it is very likely to jeopardise the entire system
* Kernel vulnerabilities are especially critical

QubesOS use a Microkernel based OS as opposed to a Monolithic Kernel based OS

* This uses a microkernel as the isolation enforcing code which reduces the attack surface
* Less code, less potential compromises
* An attacker must be capable of subverting the Xen hypervisor itself, in order to compromise the whole system
  + Which is harder to do than on a type 2 hyper visor like VMware or VirtualBox
  + No full host OS to compromise with a type 1 Hypervisor (Bare Metal) like QubesOS

**System Architecture**

Enforces security domains through different VMs

* Different apps will be opened in separate VMs
* The GUI domain, ‘Dom0’, creates the desktop and gives the illusion that all tasks are being executed natively on the desktop
  + However, they’re happening in separate VMs
  + Dom0 also isn’t connected to any network
* Good idea to have the network (VPN) running through a separate VM, like Whonix, and tunnel all the other VMs through the network VM
  + This means that any attacker who compromises the network VM would also have to find a way to escalate their attack to the other VMs too

No host OS used as Xen is the bare metal hypervisor

Can open any file as a disposable VM

* Can close and delete VM leaving no trace

USB VM protecting you from malicious USBs

* Data can then be safely transported safely to other location VMs

Secure copy and paste between VMs

Secure networking between VMs and the internet

Built-in integration with TOR

**Weaknesses**

**Lack of hardware support**

Needs a CPU that supports virtualisation tech

* Intel VTD or AMD-v

A lot of RAM

Performance & app compatibility

**You can use a live USB/CD version to test if QubesOS will work on your laptop**