**Operating Systems**

Hardware 🡪 OS 🡪 Applications 🡪 User

OS has full control of all application on a device, if the OS isn’t secure or is compromised, then it is game over from the start.

**Windows**

Bad track record for weak security design

More recently they have started to take security a lot more security

Tracking and privacy issues still

**Mac OS**

Strong security features

Compared to latest windows 10 however, it actually has less security features and less 3rd party security applications

* Limited choice of security features for MacOS

**Linux/BSD/UNIX like**

* CubesOS
* Debian
* Tails
* ArchLinux

Very security and privacy focused OS’s

**iOS**

* Extremely secure
* Closed OS
* Limited to what you can do and change but more security comes with that

**Android**

* Always upgrading security features but not as strong as iOS
* Open OS
* Nearly unlimited with what you can do and change but this isn’t always good when it comes to security if not used right

**Security Bugs & Vulnerabilities**

Security features aren’t everything when it comes to the security of an OS

We care about our actual risk in the real world

* One way to look at this is to look at the security bugs and vulnerability history
* **CVE details**, security/vulnerability database for most OS’s

“Buying into the Bias: Why Vulnerability Statistics Suck”

**Usage Share**

How popular is the operating system you’re using

81% of the total desktop OS market is Windows

**40% are still WINDOWS 7** (very exploitable)

Smartphones have now jumped the creek with them now being the most used form of computer in 2018 (51.49%)

These show the bigger or biggest targets

Androids need to be constantly patched, especially since they are becoming the most popular OS