Mobile Operating Systems

Now that we've covered desktop operating systems in the previous lesson, I'm sure you're wondering what options you have for * ***hold iPhone and Android device*** * mobile operating systems. Well, we're pretty limited here. On the bright side: it's a shorter lesson.

It would be even shorter if you didn't have these promos, so get the course on Udemy...

Promotional Spot

Very similar to desktop operating systems, everything you do on your mobile devices runs on top of the operating system--*like iOS or Android.* You're not going to be accomplishing much in this course if you're on an inherently insecure and unprivate OS.

Let's start with the most popular, open source, operating system, *Android.* Android is difficult to analyze because vendors have the ability to modify the OS, or ROM, to their liking, causing a lot of variance between different devices. *OnePlus, the Chinese budget phone manufacturer uses their own version of Android called OxygenOS, which in October of 2017 was found to be collecting data about user's activities, tying the data to their serial number, which can then be tied to the individual who purchased the device. On the other hand, Silent Circle manufactured the BlackPhone 2, which was built from the ground up to be an extremely secure and private version of Android.* These two companies took Android's openness in two entirely different directions. So how do we analyze this? Well, I've split Android into three separate types, making it easy for you to understand the key differences.

Type 1, the most common form of Android, is modified and skinned, from a manufacturer like *HTC, Samsung, Motorola, or OnePlus*--just to name a few. There will be exceptions, but in general, the security is alright. *It fluctuates, but Android is typically more prone to vulnerabilities than iOS. Even Samsung's Knox software, which is made to improve the phone's security, had three vulnerabilities that affected Knox version 1.0-2.3. Additionally, the Google Play Store has suffered many more malware attacks than iOS, and has significantly less apps that are NSC compliant, versus Apple's ATS compliance, I'll leave a link to this great post talking about compliance, since it's a complex subject I won't be covering due to time restraints. Additionally*, *it takes these third-party manufacturers time to receive security patches from Google, who develops Android, and make compatible with their own versions of Android. This means you're getting delayed security patches on your device.* To top that all off, lots of manufacturers and cell providers like Verizon *install their own apps that aren't removable and increase the risk of exploits and/or privacy invasion.* Speaking of privacy, most manufacturers implement some form of additional tracking on these devices, as seen by *OnePlus, Motorola, HTC, and possibly Samsung.* Keep in mind that Android is tightly integrated with Google on Type 1, so you're being tracked by *Google, the manufacturer of your device, and possibly the cell provider you purchased the phone from.* You are being screwed here.

Type 2 Android is more commonly known as stock Android, which is what Google pushes out on their phones. For security, this is definitely an improvement from Type 1. *Google pushes out consistent security patches that don't need to be cleared by third parties.* But, there is still a higher risk than iOS because of the poor compliance on the Google Play Store. Type 2 also limits the amount of preinstalled software, and cell providers won't install anything--assuming you buy the phone unlocked directly from Google. This is much better than Type 1, but it's not perfect. Type 2 is tightly integrated with Google, making it very poor for your privacy, but at least only one company has your data.

Type 3 Android are custom ROMs. Custom ROMs can be installed on most Google and OnePlus devices very easily. As for other devices, cross your fingers for luck. The beauty of custom ROMS is they give you the ability to install a variant of Android that favors your security and privacy. The standout project at the moment is *LineageOS, which is FOSS and built to protect your data. It adds tons of privacy features, allowing you to view and block hidden app permission requests, it doesn't dump location data, and it has many other security and privacy precautions not found in most ROMs.* Additionally, it comes with no Google services, meaning no third party tracking. This also means there is no Google Play Store, so there's no risk of malware from there, yay! But how do we get apps? Well, there's the *F-Droid Store, a store that only hosts FOSS applications. If you need an app not found on F-Droid, you can manually install an app yourself, or use the Aurora store from F-Droid. If you still need the play store, or want some Google Services, you can install gAPPS on your ROM that correspond with the Google features you need, so you have full control of the entire process.* If you're running a good custom ROM like Lineage, that is properly configured without Google, you're getting some of the absolute best security and privacy for your mobile device, making Type 3 Android king.

Let's move over to iOS. Apple's security is very strong, mostly because of their heavy app requirements from the App Store and general locked-down nature of the OS. *iOS will almost always beat Type 1 Android in security and privacy.* Now, comparing iOS to Type 2 Android is tough because they're similar in many ways. *They're both managed by the company who creates the software and hardware, there's little bloatware, security is good, and both are companies who perform* *background data collection, although Apple is typically considered better than Google. Between those two, you need to make the call over what company you trust more with your data.* Lastly, there's iOS versus Type 3 Android, running a custom ROM like LineageOS without any Google services installed. There is very little room for debate here, *Type 3 Android is almost always considered better than iOS in almost everything we are looking for in an operating system,* including true FOSS that isn't directly managed by a central company.

As a side note, avoid rooting and jailbreaking devices, since it'll open up your device to malicious activities. *There are scenarios where rooting and jailbreaking can be beneficial for us, but most of you should avoid it unless you know exactly what you're doing.*

As for other mobile operating systems…*Windows phones are for the most part dead, and we know their privacy and security doesn't stack up. Blackberry, is still alive? With extremely good security. You will also get some security through obscurity because of their scarcity, as discussed in the last lesson. But, keep in mind that Blackberry is far from a private company, so custom ROMs will still beat it there.* The last device to mention, which is still in development at the time of making this lesson is the *Librem 5, a phone built on the Linux distribution Debian. This is an amazing project, but it hasn't been released yet, so we'll see how it does. They also say on their website you'll be able to install custom ROMs like Lineage on the Librem, so that's neat as well.*

To summarize, if you're a user who draws your convenience line pretty early on, I would recommend iOS or a stock Android device. But, if you're willing to go above and beyond and get a truly private and secure device, you're going to want to check out Type 3 Android, preferably without Google services, and hopefully one day the Librem 5 will also be a good option--I can't wait to review the device!

Queue Outro Promos

That's going to finish the main options for a private and secure experience on your mobile devices. It's not as simple as I originally envisioned, but the final choices really distinguish the direction you may want to head. I hope this was useful, and I'll see you in the next lesson, where I'll teach you about *expendable OS's, li*ke virtual machines and live operating systems. See you then and thanks for watching!