Marlowe Cosby Jr.

Old Dominion University

COVA CCI Undergraduate Research

Title: How secure are Android and Apple's operating systems and based applications against cyber attacks and cyber crime

.

November 20, 2021

Supervised by:

Kazi Aminul Islam

Research Assistant Professor

School of Cybersecurity

Old Dominion University

I. Abstract

Smartphone has become an important part of our everyday life. Android and apple are the two most used operating system (OS) for smart phones. We usually store important information in our smart phone, e.g.: credit card, bank account, driving ID, SSN. As a result, Android and Apple operating systems and applications have both been subject to a wide number of vulnerabilities and attacks. This directly effects many people being that they are the global leaders of users within their platforms reaching billions of people daily. It is important that smartphones receive better defense and security. In this paper, we aim to analyze the defense structures in place for both operating systems, possible solutions, and compare the two and examine if one is truly more secure than the other. Android and Apple both have not been as secure with their operating systems as expected leaving many users exposed to cybercrime.

II. Introduction

As technology continues to grow and develop so does cybercrime right along with it. In the process, the advancement of cell phones has only become smarter. Phones now can contain nearly a person's entire life, from banking to medical records to any other important personal data and information. While this can be seen as a great thing it is also very dangerous and can end up leaving people in shambles if not properly secured and protected. Over the years both Android and Apple operated systems have been attacked numerous times due to vulnerabilities in their defense. As a result many people have ended up losing money, personal data, and info and more. With over five billion mobile users in the world, nearly 4 billion are Android users, and a little over 1 billion are Apple users (Stevanovic). As technology continues to grow, Apple and Android both need to do a better job of keeping their systems, software, and customer data secure. In this study, I analyzed both the Android and IOS based applications and operating systems. Explaining how they operate and defend against cybercrime, analyze their defense structures, and evaluate if one is more secure than the other. The purpose of this study is to not only understand how both operating systems work, but also what makes their system work, and what specifically in each system is most vulnerable, or being taken advantage of. We also organize the vulnerabilities of android and apple OS and discuss some of the possible improvements for each OS.

First topic

a. Comparisons of recent attacks on IOS & Android applications, operating systems

It doesn't matter what mobile operating system you are using, both Apple's operating system and Android can be equally vulnerable to social engineering attacks, and or phishing attacks (Norton). From phone calls looking to obtain verbal information to emails looking for you to enter in personal data or click a link to malware. Many users find Android attractive because it is an open-source operating system. This means the code to the operating system is open for public use, people can essentially see the blueprint to an extent and use that information however they would like. What most users aren't aware of though, is that you need to be even more cautious on open-source operating systems. Downloading a rogue, off market untrusted app is the easiest way to infect your Android phone, tablet, or wearable device with malware or a virus. The same is true for Apple operating system as well, especially if you download an app from a third-party source. It just happens less frequently within the Apple operating system due to their strict security along with its closed source code. That's why it's important to download apps only from reputable sources, like the google play store and or apple store (Norton).

In an experiment conducted by Nurhayat Varol, he was able to successfully hack into the android devices via frequency-based attacks, and application-based attacks. Also, Varol was able to develop the software called "Primary Mobile Hack Builder" to control Android phones running android operating system from a distance using frequency-based attacks. Using a basic software-based radio circuit worth under ten dollars, they were able to access text SMS messages on the device, locate the device, listen to the device, and even take photographs with it as well and control its camera (Varol). The amount of possible monetary damage simply cannot be measured, the ability to do such damage to this platform with under ten dollars is absurd. Androids defense against these types of attacks need a lot of work done in order to continue to prevent things like this from happening, much more work needed in this specific area by far in comparison to Apple's operating system.

b. Vulnerabilities of each OS

The Android operating system is widely used across businesses and is very popular. Developers are constantly building new apps designed to run on the system. There is an app review process for Google Play. Unfortunately, the process is far less strict than what developers face when adding apps to Apple's App Store (Norton). It's an easier process for malicious apps

to sneak onto the Google Play store and easier for users to end up installing one. One of the main issues is that the end user, the customer or user of the device can go into an Android device and enable the installation of software from anywhere online, untrusted sources (Norton). The software usually is an APK, or Android Package Kit. It is an assortment of files that can be downloaded and installed from a website bypassing the Google play store review (Norton). Android owners can modify the source code of their Android devices since it is on an open-source platform. While this does favor users who want the flexibility to change the way their mobile devices run, it can make Android devices vulnerable to attacks. When altering their device's source code, users could accidentally leave an opening for cybercriminals, and likely wouldn't even be aware of what they have done.

Unlike the Apple's operating system that only runs on Apple-branded products, the Android operating system runs on mobile devices manufactured by a host of companies (Norton). This also is a very good reason that they are targeted more and face more issues, being that they simply are across many different devices. Some companies might provide hardware that is more secure than others. The manufacturer of the device can use custom read only memory or base operating system that has software installed that cannot be easily removed or analyzed for malicious intent (Norton).

Apple's operating system has stricter controls as it is much more difficult for developers to get apps into the App Store (Norton). That's because the review process is highly strict and allows much less than Android. Because of this, it's less likely for a malicious app to appear onto Apple's store. Although, Apple doesn't allow the owners of its devices to modify its iOS operating system or custom read only memory chips to be loaded on their devices. That makes the system more secure since Apple controls the complete experience (Norton). This doesn't stop some owners from "jailbreaking" their Apple mobile devices or modifying their source code. Jailbreaking has been around for years but essentially is modifying the software in order to install unauthorized files. But jailbreaking has also become less relevant nowadays as well. Jailbreaking opens new capabilities on the devices that may be an upgrade to some but really isn't worth the risk if damage that would come from it. If a product becomes jailbroken Apple won't provide any support. Because the iOS operating system powers fewer mobile devices, hackers don't target the system as often (Norton). Hackers and cybercriminals can ensure more

victims if they focus more of their attacks on the more popular Android operating system, with a much wider selection of devices as well.

In a study by Jalal B. Hur, and Jawwad A. Shamsi, they found that there are various malware that already exist for Android Smartphone in market which might lead to different type of attacks. Also found that security issues in Android based Smartphone have become even more severe because of vulnerabilities in the Android design. One large vulnerability found was Androids SSL/TLS implementation. They found it to be not only very inadequate but also highly permissive. SSL/TLS serves as the encryption services between the communications of a client and server, allowing this to be vulnerable is highly dangerous for all parties involved. During their analysis of Google Play marketplace there were more than 4,000 applications that take credentials and data for bank accounts, e-mail accounts, and social media accounts (Hur). Due to poor SSL implementation in third party application, there are over 185 million users that could be affected (Hur).

Ranganath & Mitra evaluated the effectiveness of vulnerability detection tools for Android applications. What they found was the existing vulnerability detection tools for Android applications are very limited in their ability to detect known vulnerabilities. They could only detect 30 of the 42 known unique vulnerabilities (Ranganath). When they started their evaluation, they had expected the Android application security analysis tools to detect nearly all of the known vulnerabilities. They had expected this because there has been a high increase of efforts in recent years to develop security analysis tools and techniques for Android applications, because of how prevalent android devices and operating system is in the business field. Almost all of the considered vulnerabilities were discovered and reported before most of the evaluated tools were last developed/updated (Ranganath). The results of the evaluation showed that most of the tools and techniques can independently detect only a small number of considered vulnerabilities. Even after putting all tools together several vulnerabilities remained undetected (Ranganath). This research suggests if current and new security analysis tools and techniques are meant to help secure Android applications, then they need to be more effective in detecting vulnerabilities.

c. Open and closed systems

Android is more so an open-source while IOS is more so a closed source. Not one is entirely opened or closed but each is either more so open or more so closed rather than more so the middle. The source code itself is the technical blueprint that tells a program how to function (Norton). Once a completed product is set for release, like a new iPhone with Apple's operating system, or an Android with Android's operating system, the creators can decide whether this blueprint will be released to the public or what parts will and wont. Being that Android is more so open-source, it directly plays a role into how people are able to manipulate it towards their own wants possibly and plays a role with how hackers identify so many vulnerabilities within the software.

Apple's operating system has long been considered the more secure of the two operating systems (Norton). Apple being the closed source it is, doesn't release its source code to app developers, and the owners of iPhones and iPads can't modify the code on their phones themselves. This makes it more difficult for hackers to find vulnerabilities on Apple operated systems (Norton). Android devices use an open-source code, and the owners or users of these devices can alter the operating system. If users decide to alter the Android operating system too much it could easily result in people creating a weakness in their own devices' security.

Second Topic

a. IOS & Android security models

The Apple operating system is considered as one of the strictest and secured operating systems for smartphones. The Apple's designers enhanced their model to reach to a model which can dispense any third-party antivirus, meaning it is very likely to automatically reject it and not even allow it to download. Their security model stands on the four pillars of device security, data security, network security, and application security (Al-Qershi). As far as their Device Security goes their model interests in saving the access of the device, creating passcodes, restricting device resources, and preventing the installation of unwanted applications or using build-in services. Their focus of data security is using a 256-bit AES encryption security technique to give Apple operating system a key advantage in comparison to android. AES 256 is virtually impenetrable using brute-force methods. AES would take billions of years to break using current computing technology. Hackers would be idiotic to even attempt this type of attack. Not saying it cannot be done but the chances are extremely unlikely (N-Able). Also, it uses two other

techniques, one being the keychain. The keychain is a process under Apple's operating system which is encrypted to save both user passwords and certificates, and the file encryption (Al-Qershi). Apple's Network security provides Secure Socket Layer Protocol v3 (SSL), Transport Layer Security v1.2 (TLS), and Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol. Those protocols all enhance the security of the communications with or through the internet and keep lines between clients and servers secure. Their Application Security is split into a few crucial mechanisms. It begins with the sandboxing of the applications. A sandbox is an isolated testing environment that enables users to run programs or open files without affecting the application, system or platform on which they run. Software developers use sandboxes to test new programming code while Cybersecurity professionals use sandboxes to test potentially malicious software (Rosencrance). Then the mandatory code signing, and the reviewing of the applications in the Apple market.

Apple's operating system in addition to these pillars also manipulate a number of security techniques as well in order to provide defense. Apple also uses Address Space Layout Randomization, also known as ASLR. It is a memory-protection process for operating systems that guards against buffer-overflow attacks by randomizing the location where system executables are loaded into memory (Shea). This randomization makes the memory vulnerability attacks, such as buffer overflow attacks more difficult (Al-Qershi). This is something android should also probably look into using, it prevents a wide range of attacks.

The developer of Apple operating system applications is required to test code into an actual Apple operating system device to see how fast it will run with different iPhone hardware. This requires an Apple Developer Certificate, doing this makes it more difficult for just anyone to do these things. Provisioning Profiles is simply an Apple eXtensive Markup Language (XML) standard file for saving the configuration of iPhone device to enable the execution of the code of a certificated developer and a list of the developer granted applications (Al-Qershi). Applications Signing is where all applications need to run in Apple's operating system to be certificated either by Apple trusted certificates or by signing in a provision profile (Al-Qershi). Entitlements is a set of privileges to be coupled with the application. These entitlements are listed as keys in the XML provision profile (Al-Qershi). Apple makes this entire process a route full of authentication and authorization requirements that must be met in order to continue. Apple also uses sandboxing in

the mix along with this as well, which is the separation between the applications installed in Apple's operating system. This technique is used with different types of applications and processes, but the interested type is the third-party applications which are the potential malicious applications (Al-Qershi). This approach utilizes from the isolation of the application containers, which are the different paths of the applications installation. In addition to all of this Apple also adds a Sandbox kernel extension over the normal Unix-based security model to enhance the security that is already nearly top tier (Al-Qershi). These are things the Android security model left out entirely, and even though it is very strict of Apple it is things like this that make their operating system more secure. The sensitive data in iPhones are protected using passcodes and some hardware encryption keys. The Advanced Encryption Standard (AES) cryptographic is implemented and two keys are used one is unique and one is globally shared (Al-Qershi). This is also a very good security technique put in place by able as well.

Android's security features are fairly different and consist of application permissions, components protection, encapsulation, memory management units, type safety, and some aspects of Linux. An application permission is the allowing/disallowing a requesting of a mobile resource such as the camera, microphone or an operation (Al-Qershi). As we saw in previously mentioned experiments conducted against Android security, these things have major flaws. There are four permissions levels; the first is "normal" (not a dangerous one and considered as an application-level permission); "dangerous" (a more risky permission could access, without the asking the user to confirm sensitive data or damaging functions); "signature" (a permission can be granted only to other packages that are signed with the same signature); and signature-or-system (a special type of signature permission that's existing to manipulate with the legacy permissions) (Al-Qershi). Android's operating system is a component-based operating system and based on the interaction between four main component types (Activity, Service, Content Provider, and Broadcast Receiver). Those components are protected from accessed by potential malicious applications (Al-Qershi). All applications in Android are archived as a package. Those packages should be signed using valid certificates (Al-Qershi). Android's process of signing is much more simple and less secure than the method used by Apple in their operating system. Android ultimately chose the route of less hassle, more ease of access along with accepting more risks and flaws in their security. Android's memory management unit is a hardware mechanism manipulated that prevents the application processes to access memory locations of the other

applications memory locations (Al-Qershi). Type Safety is a programming aspect that Android ensures to prevent the attacks which targets buffers and memory. Using programming language such as Java which is considered a type saved language and using an Android binder to communicate with different languages are aspects to ensure this mechanism (Al-Qershi). Android's operating system inherits some security aspects from the Linux which is built from. Two basic mechanisms are inherited, the Portable Operating System Interface (POSIX) which creates sandboxing to protect different applications from conflicting and interleaving with each other (Al-Qershi). Here we see Android's use of sandboxing is slightly different than Apple's in such a way they use a simpler POSIX route rather than their own traditional route or procedure. The second aspect is the file access which is the well-known security access lists to manage the users and files accessing and preventing an illegal accessing. Android seems more concerned with big picture ideas and security rather than the smaller things that can matter later on or cause great damage from a lot of work even though it may seem small.

b. What makes Android so attractive to cybercriminals vs IOS

The global popularity of the Android operating system makes it a more attractive target for cybercriminals, not just the open-source code alone. Android devices are more at risk of the malware and viruses that these criminals unleash (Norton). While Apple's operating system may be considered more secure, it's not impossible for cybercriminals to get into iPhones or iPads. The owners of both Android and Apple's operating system devices need to be aware of possible malware and viruses and be careful when downloading apps from third-party app stores (Norton). Also like I have previously stated before as well, Android's operating system is across a much wider number of different devices that all are unique and also is used more so in the business sector which itself is a great target as well. Android meets nearly every checklist a cybercriminal has in comparison to Apple, more possible devices to manipulate, open-source code, used most in businesses etc.

Third Topic

a. The defense infrastructure of IOS applications and how it combats ransomware

Christian D'Orazio demonstrates how their previously published adversary model for digital rights management (DRM) apps can be used to detect vulnerable Apple operating system devices

and to analyze (non-DRM) apps for vulnerabilities that can potentially be exploited. Digital Rights Management itself is just a way to protect copyrights for digital media, in this case we are talking about applications. Using said adversary model, they investigated several jailbroken and non-jailbroken Apple devices & applications. Those being the Australian Government Medicare Expert Plus (MEP) app, Commonwealth Bank of Australia app, Western Union app, PayPal app, PocketCloud Remote Desktop app and Simple Transfer Pro App. They were able to exploit these apps via jailbroken apple operating system devices. These apps are very commonly used and crucial to the everyday life of a user, from finance to health and important data and files. They also were able to demonstrate how the identified vulnerabilities can be exploited to expose the user's sensitive data and personally identifiable information stored on or transmitted from the device. Using Disassemble and Debug capabilities, being able to static analyze an app at run time, an attacker could recover the binary code to be used in subsequent exploitation (D'Orazio). Security mechanisms enforced by Apple such as app encryption will continue to be bypassed cybercriminals if these security mechanisms are not strengthened. Christian D'Orazio concluded with several recommendations on how to enhance the security and privacy of user data stored on or transmitted from these devices.

III. Conclusion

a. What can be done in the future? How could both sides improve security?

In conclusion, Apple based applications show to be less of a target to cyber attacks due to cybercriminals finding more ease within finding and exploiting vulnerabilities within the Android operating system. Android being the operating system for countless different devices it is very hard to be able to keep all secure as possible. Android walks with a giant target on its back being the most used operating system in modern businesses, along with having an open-source code. Apple being the more so "exclusive" one could say is able to be closed source and only run its operating system on a handful of devices in comparison to Android. If Apple and Android switched places maybe Apple could do a slightly better job but something of that nature is highly unlikely and probably won't happen. Due to the circumstances Android deals with it is fairly clear Apple in general is the more secure operating system with their strict rules and regulations.

Android should investigate how to make their operating system equally as secure across the many devices they power. Android may also want to look into a possible shift into if not closed source code, to a more so middle ground area rather than their current state of open-source code as well. Android could investigate using Address Space Layout Randomization if they can handle that with the amount of data they have. Apple had a large issue with jailbreaking in previous years but now it has gone down drastically as they have improved upon their security and defense immensely putting them into a tier of their own.

From Christian D'Orazio's study we can see that Apple's application encryption is something that needs to be improved upon as well. The security and privacy of user data also is something they need to improve upon as well as it is stored on or transmitted from these devices, and always the main target usually. In 2013 there were over 7 million Apple operated systems that were jailbroken in one week alone. Their security and defense had failed greatly, and people were easily altering the system and device (Kovach). Today less than one percent of Apple operated system devices are jailbroken (Hanley). That is nothing but their incredible security measures and defense structure put in place. While both sides do have areas to improve on, Android has a bit more work cut out for them while Apple seems to be doing fine in recent times. If the two both put their teams together, I believe they could eliminate if not all nearly every vulnerability both sides have and both security structures would be benefitted. Generally, Apple's operating system and iOS-based applications are more secure than Android. What I achieved from this study is a much more profound understanding of not only Android and Apple's operating systems and defense, but also a better understanding of the mindset of a cybercriminal as they attempt to break into these platforms. In the future, I expect Apple to continue as the more secure operating system and secure applications, but I also expect Android to greatly improve.

IV. References

"Advanced Encryption Standard: Understanding AES 256 - N-Able." Understanding AES 256 Encryption, N-ABLE, 9 Apr. 2021, https://www.n-able.com/blog/aes-256-encryption-algorithm.

Al-Qershi, Fattoh, et al. "Android vs. IOS: The Security Battle." 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 2014, https://doi.org/10.1109/wccais.2014.6916629.

"Basic Computer Skills: Open Source vs. Closed Source Software." GCFGlobal.org, https://edu.gcfglobal.org/en/basic-computer-skills/open-source-vs-closed-source-software/1/.

D'Orazio, Christian J., et al. "A Markov Adversary Model to Detect Vulnerable IOS Devices and Vulnerabilities in IOS Apps." Applied Mathematics and Computation, vol. 293, 2017, pp. 523–544., https://doi.org/10.1016/j.amc.2016.08.051.

Hanley, Mike. "Duolytics: Half of IPhones Running Most Secure Authentication Scheme." Duo Security, 26 Feb. 2016, https://duo.com/blog/duolytics-half-of-iphones-running-most-secure-authentication-scheme.

Hur, Jalal B., and Jawwad A. Shamsi. "A Survey on Security Issues, Vulnerabilities and Attacks in Android Based Smartphone." 2017 International Conference on Information and Communication Technologies (ICICT), 2017, https://doi.org/10.1109/icict.2017.8320163.

Kovach, Steve. "7 Million IPhones and Ipads Have Been Jailbroken This Week Using a New Hacking Tool." Business Insider, Business Insider, 8 Feb. 2013, https://www.businessinsider.com/7-million-people-jailbreak-ios-2013-2.

Rafter, Dan. "Android vs. IOS: Which Is More Secure?" Norton, 2014, https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html.

Ranganath, Venkatesh-Prasad, and Joydeep Mitra. “Are Free Android App Security Analysis Tools Effective in Detecting Known Vulnerabilities?” Empirical Software Engineering, vol. 25, no. 1, 2019, pp. 178–219., https://doi.org/10.1007/s10664-019-09749-y.

Rosencrance, Linda. “What Is a Sandbox? Definition from Searchsecurity.” SearchSecurity, TechTarget, 23 Sept. 2021, https://www.techtarget.com/searchsecurity/definition/sandbox.

Shea, Sharon. “What Is Address Space Layout Randomization (ASLR)? .” SearchSecurity, TechTarget, 23 June 2014, https://www.techtarget.com/searchsecurity/definition/address-space-layout-randomization-ASLR.

Stevanovic, Ivan. “The One OS to Rule Them All - 33 Android vs IOS Market Share Stats.” *KommandoTech*, 14 Dec. 2020, https://kommandotech.com/statistics/android-vs-ios-marketshare

Varol, Nurhayat, et al. “Cyber Attacks Targeting Android Cellphones.” 2017 5th International Symposium on Digital Forensic and Security (ISDFS), 2017,https://doi.org/10.1109/isdfs.2017.7916511.