Smartphone and Security Issues

Ahmad Vakil
The Tobin College of Business
St. John's University
Queens, NY 11439
USA

Abstract

The popularity of smartphones around the world during the last fifteen years has increased significantly and users of these devices now face a tremendous challenge in order to access, store, and disseminate information safely. Although smartphone sales have reached a saturated stage, the sheer amount of smartphone models still introduced to the market remains impressive. Furthermore, new smartphones have become more and more powerful with additional functionality. As a result, users of such devices utilize them to process more sensitive personal, financial, and even corporate data and information. Indeed, the huge amount of information and the quality of such information processed by these devices presents us with a challenging security task. Smartphone security threats are now making headlines every day, and they are continuing to become more of an issue. In this study, we first examine major trends in smartphones technology. Then, we focus on major vulnerabilities of these devices during the last three years. Based on our examination, it can be concluded no smartphone is totally safe from all attacks. However, we make some recommendations in order to alleviate some of the security vulnerabilities of smartphones and lead to a more secure mobile device.

Keywords: Smartphones, Operating System, Security Vulnerability, and Malware.

I. Introduction

A "smartphone" is defined as a mobile phone that performs many of the same functions of a computer [1]. It is typically controlled through a touchscreen interface and runs with the use of an operating system that allows internet access as well as the download and use of applications, commonly referred to as "apps." Mobile phones were first invented in 1973 by a Motorola employee, and consisted of a much larger unit than we see today. The phone weighed close to 2 ½ pounds, a drastic difference from the mere ounces that most phones now weigh [2]. The construction of the first-generation cellular network began in 1979, and the first consumer mobile phone was released in 1983. These phones and networks continued to develop and adapt over the next thirty years as they grew to be a common communication device of most households in addition to existing landlines. Construction on the second-generation cellular network began in 1991. Cell phones continued to develop and became far more advanced, and in 1992 the first "smartphone" was released by IBM [3]. The term "smartphone" was coined due to the fact that the device was "smarter" than a regular phone and could complete additional computing tasks rather than just placing and receiving calls. Just as with the original mobile phone, the sale of smartphones began to rise rapidly each year as their processing power continued to increase exponentially. Information today is available at the blink of an eye on smartphones, and ease of access has never been greater. Rather than having to take a trip to the library, or conduct a lengthy search of an encyclopedia, a smartphone can be used to quickly browse the web and locate the answer to almost any question in seconds. The abundance of information on any topic is staggering and humans have become more and more dependent on these devices to access information instantly at almost any time and from anywhere.

The phones have come a long way from when they were first invented and until recently, the market for smartphones expanded each year. People who did not own phones were purchasing smartphones, and people who owned regular cell phones were often upgrading to smartphones. As figure 1 shows, the upside trend continued on for several years, but recently the number of smartphones sold has started to level out [4]. Over the past three to four years, the majority of the market for smartphones has switched to customers who purchase them to replace their existing unit, rather than upgrade to a smartphone for the first time. This is not to say that the market for these phones has disappeared completely, but the market has entered its saturated stage.

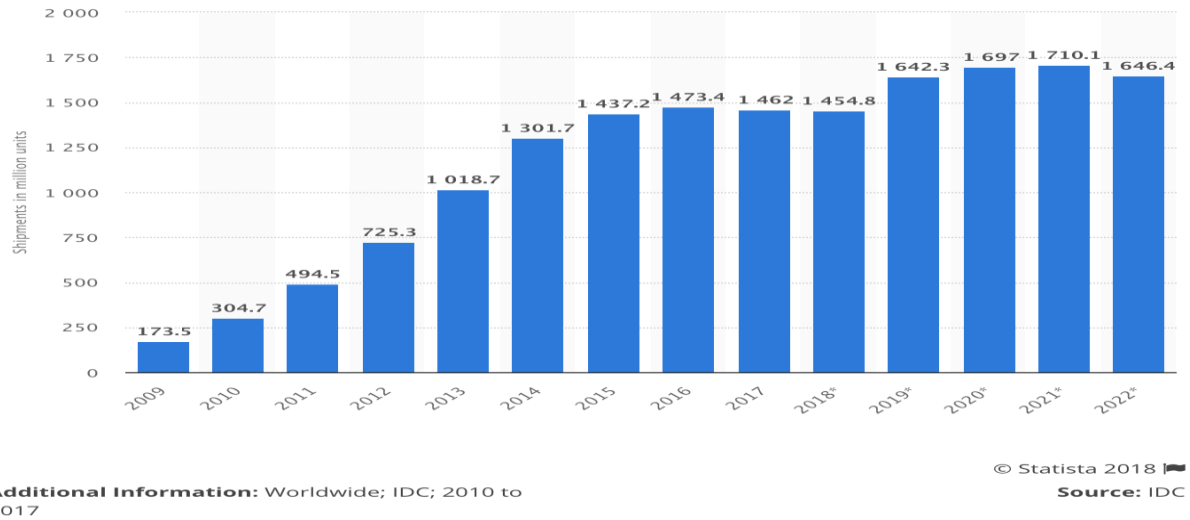

Figure 1. Growth of Smartphones Worldwide from 2009 to 2017 and Estimate for 2018-2022.

Users of smartphones are connected to each other at all times of the day or night. People use them for everything from watching television to setting an alarm that wakes them up in the morning. However, this increase in connectivity and number of smart-devices has also brought along a darker side to it: security threats. Smartphones today contain immense amounts of assorted data such as contacts, emails, photos, text messages, e-mails, calendars, fingerprints, passwords, credit card numbers, bank accounts, and more. This means that they are a very lucrative target for attackers, as there is often much to gain. In addition, computers have become increasingly hard to successfully attack in recent years due to increases in security. On the contrary, the security of many smartphones has started to lag behind, as attackers have found new ways around the often-outdated software. This has attracted a larger number of attackers as many of them figure the easier the attack the better, and smartphones are certainly easier to attack than computers. To make the problem worse, some older devices may still contain different types of security flaws that were never fixed, presenting a huge liability for the owner. In addition, a stolen or breeched smartphone would likely cause massive problems for any owner. This is especially amplified with a business' devices, since at this day and age it is not uncommon for a business to give their employee a smartphone to use for professional scenarios. Lost data can cause any individual or company a large amount of time and capital. Consequently, every device is always vulnerable in some regard and the proper steps must be taken to ensure data security. Some companies devote their time to securing smartphones with security software and hardware to try to prevent this data loss. However, more and more mobile security threats are both discovered and created every day and it is critical to understand vulnerabilities for these devices. It is important to know what to look for, and what to avoid when it comes to smartphone security threats; as well as how smartphones security has changed over the recent years after dealing with different types of attacks. The smartphone has dominated the way life is lived in the 21st century and it is now a key part of society. One of the main issues to point out is that the security of a smartphone depends on the type of operating system that it is running on.

2. Background

A battle for the superior smartphone operating system has commenced and it also consists of two popular options. One main choice is Android, which was created by Google, with the other foremost possibility as iOS, which is distributed by Apple. The Android system was developed by Google starting in 2005 when they purchased Android Inc. and became available commercially for the first time in 2008, when the HTC Dream was released [5]. Android is an open-source platform that allows a large amount of customization and user input. The software was continuously refined and improved. The other leading option for smartphone users is iOS-based Apple phones, also known as iPhones. Many users of the iPhone used Apple machines in the past and felt comfortable with how their devices operated and their similarity to Mac OS. Two of the top devices released in 2018 include the iPhone XS Max and the Samsung Galaxy Note9 [6]. They both come with storage ranging from 64 Gigabytes to 512 Gigabytes, about a 6.5-inch screen size, multi-core processors, and multiple cameras and microphones built into them. A closer look at market share as of April 2019 can be helpful [7].

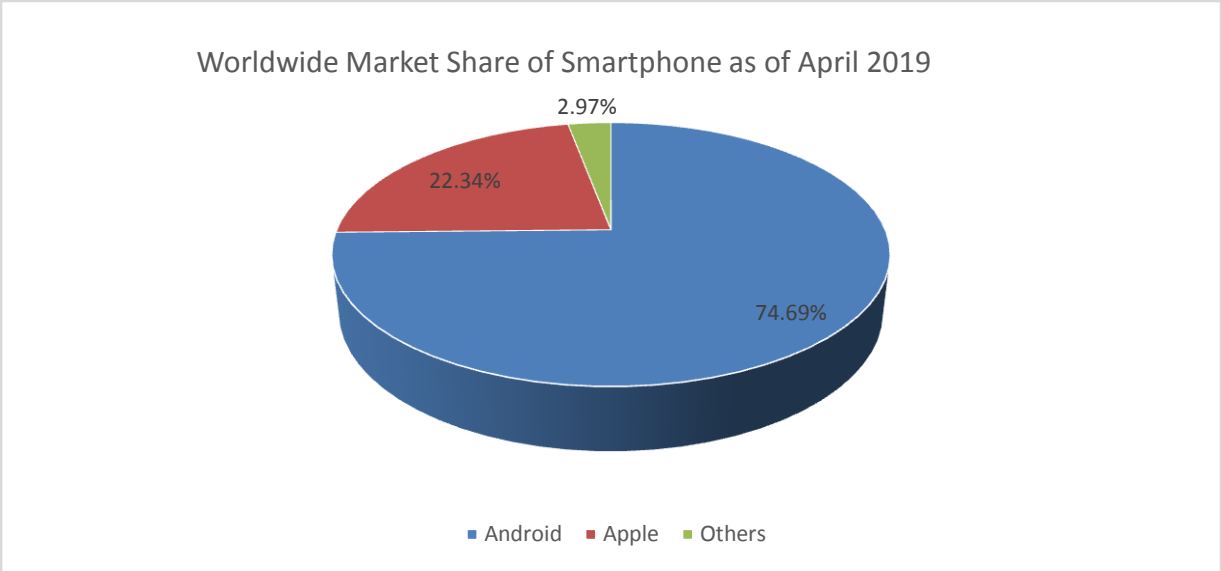

Figure 2. World Market Share of Smartphone as of April 2019

As Figure 2 shows, worldwide Android leads the market with about 74.69% of the market share, while iOS is next behind at about 22.34% of the market share. These two operating systems accounted for more than 97% of the market share. As of April 2019, Apple devices are far more popular in the United States with a market share of 52.95% while Android has a market share of 43.94%. Most smartphones released today have a sizeable amount of processing power that would compare with regular computers just a few short years ago. In addition, smartphones today come in 128 Gigabyte or 512 Gigabyte storage options, which is what many laptops still contain as the size of their hard drives. It is remarkable how far technology has come and how our computing power continues to grow bit by bit every day.

3. Discussion of Security Flaws of Smartphones

Smartphones over the last ten to fifteen years have evolved greatly and they now store more sensitive information than ever before. The wealth of data that can be found on almost any smartphone is astronomical and much of the information can be sensitive. This has caused an increase in both the number of attackers and the amount of attacks that take place on a day-to-day basis against mobile devices in general and smartphones in particular. It is a growing cause for concern and security is of the utmost importance for any smartphone on the market today.

In order to accurately compare the security issues of smartphones, it is important to direct the reader's attention to how the two largest smartphone operating systems (iOS and Android) approach security. In particular it is first necessary to discuss how the two units view the interaction between software and hardware. The traditional mantra for technology companies that manufacture computers is to ensure their systems and products are interchangeable. This way, hardware companies such as Samsung can make products that are not dependent on any one particular software, and software companies such as Google can develop programs that are not contingent on any one particular hardware. On one hand, this separation of powers provides an inherent benefit to both parties as they can focus on creating more specialized products and providing value in different domains. On the other hand, this separation of powers creates an environment for possible vulnerabilities since there are so many variations of hardware devices and software programs which can be manipulated by hackers and malicious code developers.

Apple Inc. however does not follow the schema. Its former executive Steve Jobs firmly believed that an integrated system in which the hardware and software are tightly linked would provide Apple with long-term stability and its customers with an optimal user experience.

Thus, it should be quite clear why Android follows an open-source model whereas iOS follows a closed-source model. If a major goal of a company is to attain a financial benefit from the exchange of a product or service, then sourcing models are provided as part of the picture of how a software company intends to achieve that goal. In an open-source system such as Android's, the source code is made available publicly for non-commercial use online. Their priority is not to sell the software to consumers but to sell the permissions to use their software to hardware companies. It is in Android's best interest to keep all of their source code available for developers to improve upon as it will provide more exposure to skilled developers who are willing to contribute to the community.

As a result of this policy the number of Android users has increased drastically during the last 10 years. Further discussion of this policy reveals how Android has become such a dominant force in smartphone operating systems. First, since Android is freely available to hardware companies, hundreds of companies have adopted the platform and were able to develop some amazing smartphones. Second, many users embrace the idea of software versatility and flexibility of Android. Third, since Android is open-source, many software developers work on developing different application programs so a huge number of application programs are developed for Android based smartphones without effort on the part of the parent company (Google).

Apple's scenario, however, is quite different than that of Android's. Since Apple produces highly integrated products, it is not in their best interest to allow their software to be open-source. Through integrating their software and hardware they have better control on all aspects of their products, meaning they can bundle them as packages. Obviously, this approach allows Apple to control all stages of production of its products. Any modification or change must be approved by Apple after rigorous testing.

It can be noted that lately, Samsung and Google have deviated from their original business model and moved toward producing more integrated products. One can conclude that this move is in response to addressing the security vulnerability of their products since an integrated product seems to have less security issues.

4. 1 Latest Security Flaws Of Android

In this section we review some of the latest security threats that android-based smartphones have experienced during the last few years. One major security threat that Android faced occurred in June of 2018 and was called the "MysteryBot" attack [8]. This attack was a spin-off of the "LokiBot" attack and was classified as an overlay banking attack. This means that the Bot would function on the screen as an overlay Trojan without the user taking notice and could steal valuable information such as contacts, keystrokes, and call logs. This attack was mainly distributed via phishing, which is a widespread malware attack that attempts to make people download the virus without even realizing it. This type of attack is often very inefficient and only a small percentage of the users actually fall for it, but they still occur every day. This attack was found on many of the same banking servers as the LokiBot, but luckily it was discovered by Google in its early stages and was patched before it could become too widespread.

In May 2018, the "GLitch" exploit was discovered by researchers and presented a huge security flaw [9]. By manipulating the electric charge sent to the memory chips in a device, this attack was able to force data corruption and gain backdoor access to run further malicious code. The exploit was a spinoff of the "Rowhammer" attack and is similar to how a buffer overflow attack functions against computers. Google was notified by the researchers of this exploit and was able to patch it by adjusting the functionality of the web browsers used on the infected devices.

Another exploit recently transpired in October of 2017 and affected a whopping 41% of all phones running the Android operating system. The KRACK attack ensued when these phones were connected to Wi-Fi, a vulnerability allowed attackers to intercept and modify large amounts of traffic being sent over the network [10]. It affected devices running Android 6.0 and up and allowed attackers to inject malware and ransom ware through different websites by altering the 4-way handshake that occurs when connecting to the network. In addition, attackers were able to steal credit card numbers, texts, photos, passwords, and emails; meaning it was a massive breach for Android and Google in general. Work was performed around the clock, and in a few short weeks of the flaw being discovered a patch was released to solve the issue.

In February of 2019, a new type of attack occurred against Android devices that turned them into crypto currency miners. Dubbed "UFO Miner", the attack was delivered unknowingly to various devices that were continuously connected to the Internet. In addition to smartphones, this attack also targeted devices such as TV set-top boxes and streaming devices. The payload was delivered through a honeypot system, meaning the device was lured in by promise of something good and then infected once the connection was established. The attack then installed a program without user knowledge which could control the system and use the processing power to mine for crypto currency. The "Miner" would consume almost all of the processing power, causing a large amount of heat and power to be produced. This would cause a large number of problems in the long run. At the moment, there is no protection against this attack besides avoiding the honeypot website and ensuring no new programs have been installed. However, if a device is infected it can be cleaned by either uninstalling the program or performing a factory reset of the device.

These types of problems are not new to Android devices as they have faced a large number of attacks over the years, testing the resolves of users. Android faces unique security challenges as their software is open-source. Additionally, the number of devices running Android is massive and it is hard to ensure that any update to the operating system will work for every model without causing any issues. Some of the cheaper Android devices (generally found outside of the United States) even transmit their data in an unencrypted manner, which is begging to be stolen by an attacker.

Android devices are more likely to contain firmware or software issues due to the sheer number of different models in existence. Google has worked hard to try to solve every issue that has presented itself in the past, but it is a tall task for them to handle.

5. 2 Ios Security Flaws

Although Apple devices are generally considered more secure than Android, it is not as if iOS has not experienced any attacks in recent years. One attack affected TSMC (a chipmaker for many iOS devices). This attack caused various problems in the production of new iPhones [11]. The attack was a WannaCry ransomware attack, which means that malware was distributed to various devices and, until a ransom sum was paid, the devices were locked and unusable. This occurred in August of 2018 and affected a very advanced technological company, effectively crippling their production. Many chips used in iOS devices had to be replaced as they were damaged or infected during this attack. This ransomware attack has affected more than 200,000 victims and 300,000 devices since it was first released and is one of the most widespread attacks of all time.

iOS devices faced another attack in April of 2018 when "Trustjacking" was discovered [12]. As a security measure a number of years ago Apple added in a "trust factor" which entailed unlocking a device and approving its connection to a computer before any data could be accessed. The device had to trust the computer in order to be able to see or modify any information on the phone. Recently however, Apple has introduced an iTunes Wi-Fi sync and this attack exploited the trust factor in a wireless manner. By simply asking the user if they trusted a device or not, there was a possibility that the attacker's device would be approved to sync up with their data and allow the theft of sensitive information. Apple combatted this by instituting a required passcode that must be entered along with accepting the trust factor in order to limit the possibility of a Trustjacking attack.

A more recent instance of attack on iOS devices occurred in January of 2019 and was called "Chaos" [13]. This attack was discovered by a researcher working to improve the security of devices so it was never widespread. Yet, it would have been problematic if it fell into the wrong hands. Vulnerabilities both in the Safari web browser and iOS would allow an attacker to execute malicious scripts and then elevate their privileges to the point that they could install an application of their choice. This application could be any type of malware and thus eavesdrop, spy, steal, commit fraud, or even crypto mine. The attack was patched with an iOS update before it ever was seen by the public so no harm came of it, though it could have been much worse. One of the upsides to iOS devices is there are a very limited number of iPhone models, meaning the company can work quickly and efficiently in order to solve many problems. It is not like Android, where there are hundreds of different types of devices to worry about compared to the ten models of iPhones today. Older iPhones contained more security concerns such as backdoor services or software issues, but almost all of them have been patched by now.

6. Steps To Improve Security Of Smartphones

With the increase in data stored on mobile phones and the rise in attacks against them, it is imperative to understand the steps that must be taken in order to ensure safe use [14, 15]. The steps will be listed first and then they will be discussed in more substance below:

- Maintain education on current attacks and vulnerabilities of mobile devices
- Ensure the smartphone is updated to the current version of the operating system
- Correctly activate and set up mobile device security apps and antivirus apps
- Download apps only from app stores or respectable websites
- Use a secure Wi-Fi network and avoid using public Wi-Fi
- Use a safe and updated browser
- Lock and set PINs on the phone
- Use reputable Virtual Private Network (VPN). Do not try free VPN services
- Update your smartphone regularly
- Use smartphone encryption features for Android based smartphones
- Only buy devices from venders who release patches quickly
- Turn off connections that you do not need
- Uninstall apps that you do not use
- Backup data and make sure it is secure.

The most important aspect of mobile device security is education. Users need to know what to look out for and what must be avoided. Different texts and calls that appear suspicious should be blocked, and any link that is received randomly should never be accessed. The latest operating systems and patches must be used.

Frequent updating of your operating system can prevent many current threats. Another option some users or companies pursue is paying for mobile security software distributed by third party vendors. Companies such as McAfee or Norton offer options for both Android and iOS devices that build on the already existing security software built into the phone. These companies offer services such as virus and malware protection, GPS tracking, media access restrictions, remote device access, remote storage, and remote wiping of devices when needed. They are generally paid in a yearly fee and can be downloaded to the device through the app store just like with any other app. Trusted sources are key in this scenario and even then links sent through text or email should be accessed very cautiously and with confirmation that the other party is legitimate. When browsing the web on a mobile device, it is key for the user to know what sites are safe and what should be looked out for. Again, operators must be extremely cautious about different links they are clicking, as it can be very easy to get a virus if the device is used incorrectly. Although it is tempting to use public Wi-Fi, however unsecure public Wi-Fi is posing one of the most vulnerable security breaches for smartphone users. Using a safe browser is another key step that should not be overlooked. Indeed, using the latest version of a secure browser is an important step to prevent security and data breaches. When the smartphone is not is use, it should be locked and only opened with a PIN. Smartphones should always have active PIN numbers and passwords to set up extra steps that must be surpassed by an attacker. The more work they have to do, the more likely it is they will be stopped from completing the attack. Simply setting a passcode to get into a phone could thwart some attacks. Using a reputable Virtual Private Network can significantly reduce online threats. Users should never install applications from untrusted sources. Another key part of mobile device security is ensuring that the phone is up to date. Both Apple and Google regularly roll out updates for their phones, and although it may be annoying to constantly have to update them it keeps the device as secure as possible at the given time. Some people go years without updating their phone, which can leave it vulnerable to many different types of attacks that have been easily patched in past updates. There are plenty of options for vendors of this type of service and the best choice is mainly preference based. For iOS-based smartphones, encryption has become a standard feature since 2009. However, it is essential that the user of Android based phone implement the encryption on his/her smartphone. Although implementing the encryption feature slows down the smartphone speed, it significantly improves the security of smartphones. Other steps the smartphone user can take to improve security are to delete unused apps and to turn off connections that are not needed. By taking these steps the phone's vulnerability will be reduced. One last step that should always be followed and should occur early on in the protection process is that devices should be regularly backed up and the data should be stored in a safe place. If all else fails, and the device is compromised or lost, this backup can be used to restore the device to an earlier time and can thus ensure that not all data is lost.

7. Conclusion

In a fairly short lifetime, smartphones have gone from a rare, novelty item to a common necessity for large number of individuals in the world. They are now incredibly powerful devices and almost anything can be accomplished by using them. They can also be dangerous, as they are susceptible to different types of attacks and contain vast amounts of personal data. Smartphone security is a leading concern for many companies and smartphone owners around the world. It is also a vital field for data security. Attacks can happen far more often than many people realize and they are quite serious. Thus, it is important to take the correct steps to secure any smartphone or mobile device and ensure their data integrity and security. From 2017 to 2018, the amount of malware attacks against smartphones more than doubled and experts predict this trend will continue to rise [16]. The sophistication of these attacks grows every day in conjunction with the amount of data that can be gained from an attack. While it is impossible to be 100% protected in this day in age, taking the proper steps and precautions can go a long way to ensure data and device security.

References

[1] https://en.oxforddictionaries.com/definition/smartphone
[2] https://www.aarp.org/politics-society/history/info-2018/first-cell-phone-call.html
[3] https://searchmobilecomputing.techtarget.com/definition/smartphone
[4] https://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/
[5] https://www.androidauthority.com/first-android-phone-t-mobile-g1-htc-dream-906362/
[6] https://www.tomsguide.com/us/iphone-xs-max-vs-galaxy-note-9,review-5741.html
[7] http://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201210-201810-bar
[8]https://www.threatfabric.com/blogs/mysterybot__a_new_android_banking_trojan_ready_for_android_7_and_8.html
[9] https://www.vusec.net/projects/glitch/
[10]https://fossbytes.com/google-android-security-patch-krack-attack/
[11]https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html

[12]https://www.symantec.com/blogs/feature-stories/ios-trustjacking-dangerous-new-ios-vulnerability
[13] https://www.techspot.com/news/78698-ios-1214-addresses-serious-security-issues-but-causes.html
[14] https://www.fcc.gov/smartphone-security/Android
[15]https://www.zdnet.com/article/android-alert-this-new-type-of-rowhammer-gpu-attack-can-hijack-your-phone-remotely/
[16]https://www.networksasia.net/article/number-mobile-malware-attacks-doubles-2018-cybercriminals-sharpen-their-distribution