Security Comparison between Android and iOS

Aman Arora
Department of Computer Science
HMR Institute of Technology
New Delhi, India

Harsh Sharma
Department of Computer Science
HMR Institute of Technology
New Delhi, India

Puneet Aggarwal
Department of Computer Science
HMR Institute of Technology
New Delhi, India

***Abstract*--- The usage of Smartphones in regular life has progressed in the recent years bringing new ways to create and transfer personal and business information. Android and iOS are the two mostly used platform among various mobile operating systems. Out of which Android users are slightly more than iOS, 1.4 billion android users and 1.0 billion iOS users worldwide at present. There are issues in the use of strong security controls in Android as well as iOS versions. This paper concerns about all the security control issues related to these two mobile operating system. This work presents the comparison between Android and iOS based on various security parameters such as communication, vulnerabilities in software, hardware, malware, resource management. It also states solutions to enhance and improve the current using parameters in the system.**

Keywords: Security; Android; iOS; Mobile Operating System(MOS)

I. INTRODUCTION

Mobile Operating System (MOS) which is a handheld operating system. This is a software podium for mobile devices which facilitates mobile devices to run the application and program. Mobile devices enable us to send text messages, browse the web, access emails and even make monetary transactions. This MOS coalesce features of a personal computer operating system and control all hardware and optimizes the efficiency. There are so many MOS in the market. The two well-known MOS nowadays is Android and iPhone Operating System (iOS). Android OS is an open source, its source code was released by Google under the Apache license which makes it accessible for everyone. The operating system is a linux based and the application software running on an application framework combining with Javacompatible [12] libraries based on Apache Harmony. Android is intended primarily for touch screen devices and the user interface is based on direct manipulation using the touch screen. The first Android phone sold in the year,2008 and the latest version is Nougat 7.1.1.

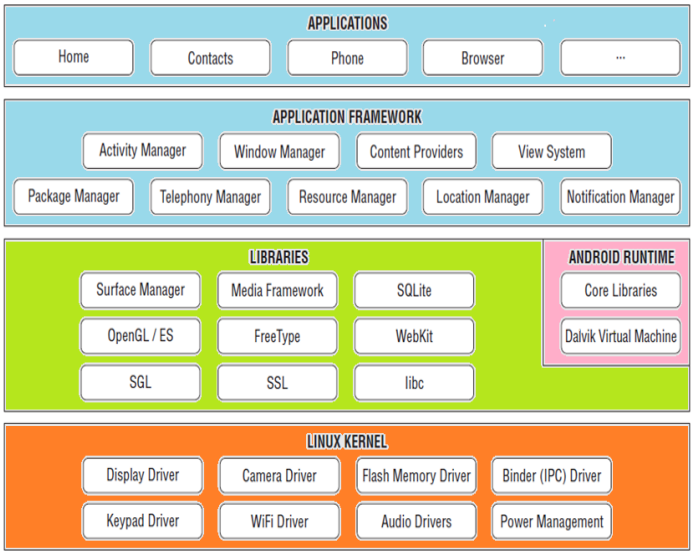


Figure 1: Android-architecture

iOS was derived from OS X . This iOS is only used by Apple Inc. for iPhone and iPad [8]. There are 4 abstraction layers which are Core OS layer, Core Services Layer, Media Layer and Cocoa touch layer. Core OS layer is the base layer of the iOS stack and assemble directly on the hardware. This layer serves a wide variety of services including low-level network access to peripheral accessories and common operating system services such as memory management policy, and thread handling file system. The iOS Core Services layer serves the establishment on which several earlier layers referenced constructed and consists of the following framework. Media layer contains the graphics, audio, video and technology geared towards creating the finest multimedia familiarity available on a mobile device. Technology in this layer were designed to make it easy for you to build applications that appears and sound enormous. The Cocoa Touch layer serves the key structure for constructing iOS applications. It explains the fundamental application infrastructure and hold up for key technologies such as multitasking, touch-based input, push notifications, and many high-level system services. Some of the application can be freely downloaded. For iOS application cannot directly communicate with other apps. The first iphone sold in the year,2007 and the latest version is iOS 10. Why we need security on MOS is to make sure all the user information is not hacked, to make sure sensitive data is not exposed to other persons and to recognize, prevent, correct and eliminate viruses.

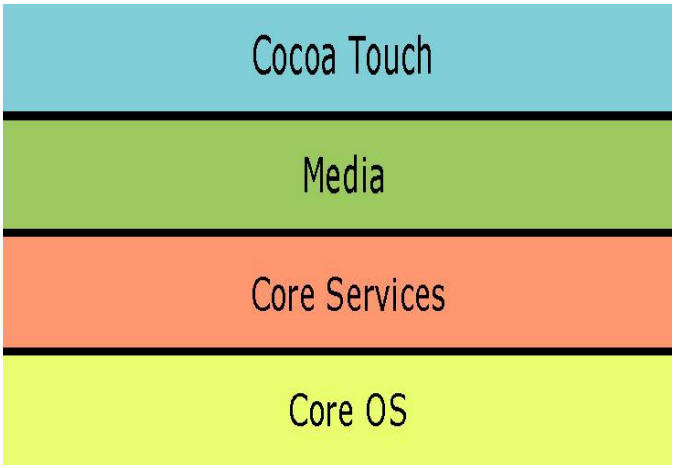


Figure 2: iOS -architecture

II. REVIEW OF MOBILE SECURITY LITERATURE

Application Sandboxing The process of application sandboxing needs declarative permissions or entitlements. These declarations are defined in the manifest of the mobile app. When a mobile app is created, the permissions or entitlements set are assigned. And once they are assigned, they will not be dynamically changed at runtime by the mobile app, or the mobile OS kernel [3]. This determines the resources that can be shared. And those limits will never extend beyond the definite declaration set at startup. This is the layer of protection that today's mobile OS provide. For mobile operating system, application sandboxing have been applied to improve the security of the mobile. Application sandboxing is a container used to manage and bound the application from accessing to the system or other application specially the malicious code and virus. Sandboxing will assign a unique ID for each application and run it as the users which run in a separate process. This is important to reduce damage by the malicious because it is isolated from the other application. For Android, the application sandboxing is based on the linux kernel platform [12]. It is a complex and robust sandbox model. Application sandboxing in Android is controlled by each application and required permission and approval to continue accessing what the application needed. This will improve and build the security tighter. Each application has its own sandbox directory and the permission is per application. For iOS, the application sandboxing has been defined by Apple as a set of fine-grained control that confines the application access to the file system, network and hardware. iOS also has a robust sandbox model where all applications shared a same sandbox model which is more secure and less open to the crowd. iOS is much better and more secured since it is only allowed users to access the system file in the root and the settings of the phone not in each application. But Android relies more on user because it required user to set the security for each application during installation time.

Data Storage Format Data storage is a place where all the data is stored either in a built in storage or external storage. Normally, a mobile device will have both built in storage and also external storage to keep all the data [6]. If storing sensitive data on a device, you need to make sure that the storage itself is secured and protected [10]. For Android, the storage of data can be stored in both data storage which is external and internal built in. External storage in Android such as SD card does not have authorization and by default all the application has read access to the storage and can read all files. Android implements standard crypto libraries to secure the storage but this method only act as password policy. With root access, it is easy for any unnecessary code to find the encryption keys in the memory. An application in Android can access all the files throughout the device without any restraint thus can spread the malware directly to the storage. While in the iOS, the devices itself do not have an external storage or memory. It only has a built in storage which requires permission to maneuver or access all the data. The Data Protection APIs built into iOS, combined with a complex passphrase can provide an additional layer of data protection. So iOS storage will be more secure than Android and make the application difficult to access the data in the data storage.

Memory Randomization Other security features are memory randomization or Address Space Layout Randomization (ASLR) [2]. Memory randomization is a process where the memory application, shared library and others in a device is located randomly. This is important to evade the malicious code or virus to attack the memory of the running application. Malicious code or virus require to find the accurate position or memory region of the task it wants to attack and this is complex for them since it have been randomly located. Even with the subsistence of ASLR, developers must take care that we extend to apply defensive programming techniques, such as preventing buffer overflow and other memory corruption that may occur. For Android operating system, memory randomization is fully applied to Jelly Bean release. For iOS, memory randomization has been applied since iOS 4.3 earlier than the Android operating system. It also added extra secured technology where iOS has code signing technology which is a process requisite to permit illegal applications running in a device. Code signing technology [1] is a process where new third party applications necessitate to be validated and signed using an Apple issued certificate. It is a compulsory process to confirm the OS is keep trusted to the new apps. It also significant to prevents the third party application from loading unsigned code resources or using self-modifying code. By right, iOS is more secured compared to the Android operating system because memory randomization in iOS is enhanced by the code signing technology.

Encryption is transformation of data into a secret code. Encryption is also the main effectual method to archive data security. You must have access to a secret key or password that facilitate you decrypt a data which is in an encrypted file. Unencrypted data is called as plain text and Encrypted data is called as cipher text. Encryption is significant for mobile operating system because it provide additional protection in case your mobile is stolen. Encryption is a new security method introduced in Android. There is no device encryption on Android version less than 3.0.

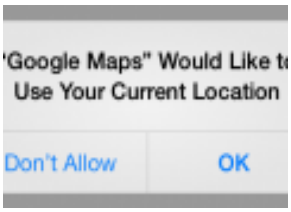
The very first encryption method for Android operating system is device encryption API which was released in "Ice

Cream Sandwich 4.0". Encryption is based on dm-encrypt (disk encryption) for Android operating system. You must have encryption pin or password [11] to read the encrypted file in Android [7]. Encryption is also a new security method in iOS too. Hardware encryption was introduced with the IPhone 3GS. Encryptions secure all our data in an Apple product. Encryption allows remote wipe by removing the encryption key for the device. Once the hardware key is removed, the device is useless for iOS operating system mobile devices. Full MDM API's available in iOS [7]. You should have passcode to study the encrypted file in iOS. Apple iOS device protection API is more robust than Android. While designing the developers does not take benefit of the encryption method although both Android and iOS operating system supports the storage of secrets in the cipher text mode on disks. All encrypted data can be stored in the form of plain text but cannot be accessed by the developers without knowing the encryption codes.

Built-in Antivirus In general there are 3 types of popular malware that affects mobile such as Virus, Spyware and Trojan [10]. A Virus is a true piece of malicious software. The Virus is usually transmitted through email. Spyware is software that gathers information about users without their knowledge. Meanwhile Trojan serves a desirable function but actually the purpose of the Trojan is malicious. Both Android and iOS mobile was introduced with built-in antivirus features to avoid malware such as viruses, spyware and Trojan from affecting our mobile operating system. Android mobile does not have a vigorous vetting process. Android users can install thousands of applications from Google Play safely. The antivirus features weren't actually found on Android devices but actually found in Google Play [8]. This means the apps downloaded from outside web source beside Google Play is very risky. The outside source is much easier for malicious applications to turn the developed software into a virus. The Android operating system will prompt a window to allow downloading some applications from untrusted web. Once permission is given, some application will download viruses into the Android operating system. The extra antivirus solution needs to be installed in the Android operating system to avoid popular malware affects our mobile operating system [6] . iOS is Apple's mobile operating system developed by Apple. Apple has done additional design work to enhance security without comprising usability. Apple does not need anti-virus program for iOS because it does not leave room for viruses to get into the system. The only place to get apps download is from the App store. Apple does not allow installation from an outside source. Everything through the Apps Store is rigorously checked to make sure it does not contain malicious codes. The iOS operating system is less likely to virus attacks than the Android operating system. Apple iOS has put forth authentication procedures to ensure safety for its users. As an open source and social network, Android is more prone to virus attached and other security threats. Recovery measures include fraud proof
susceptibilities in privileged programs by implementation monitoring (ARSP)
ARSP project [2] worked on recognition of susceptibility misuses in privileged programs by monitoring operational audit traces. Their work is based on the hypothesis that privilege programs are more likely to deed susceptibilities. They have presented the Program Policy Specification Language based on a modest predicate logic and regular expressions.

III. METHODOLOGY

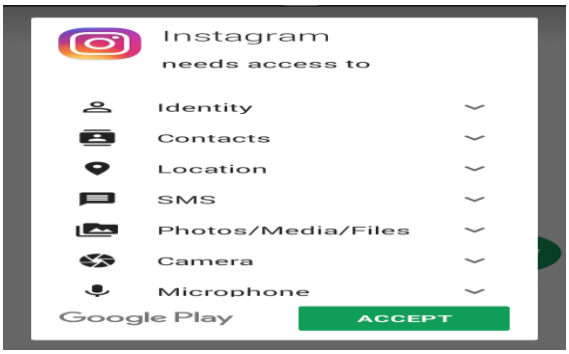
This study used the descriptive method of research using documentary examination to gather significant information and to meet up the goals of the study. For this purpose, the proponent used the Internet, scientific articles, threat reports and recorded presentations as sources. To get some base knowledge about risks and threats for applications the proponent looked into security motivation, architecture, malicious history, malicious approaches, threats and vulnerabilities.The proponent used a questionnaire checklist as a survey instrument to determinethe level of security awareness and practices of Android and iOS users.
Apple has a good reputation for staying on top of security. The company strictly reviews all of the apps available through the App Store to avoid allowing malware through. They also work hard to ensure devices have the most recent version of the iOS installed (which usually includes security updates) and encourage mass upgrades. Because of their reputation and overall popularity, breaching Apple's iOS would be an impressive feat for any hacker. But still last year, security researchers found a vulnerability that had the potential to allow fake versions of apps to get into iOS devices. More recently, the company discovered 39 malware-infected apps in the App Store; this was considered to be Apple's first major cyber attack. Additionally, in September, 2016 it was discovered that more than 225,000 iPhone users had their Apple account information compromised by malware. This attack only targeted individuals with jailbroken iPhones. Jailbreaking allows people to customize their phones in many ways, but it also makes them vulnerable to hackers and voids Apple's warranty.



Built on an "open" philosophy, Android makes it easy for users to configure the OS to their personal preferences. Many Android users say they love the flexibility and the option to customize their devices.
Unfortunately, keeping things "open" is also what keeps Android more vulnerable. Android-based phones are more widely used across the world, and studies have shown that a much larger percentage of mobile malware targets Android over iOS.
When it comes to OS updates, Android is notorious for being inconsistent. It is not uncommon to find an Android owner running an old version of the OS on their device, making them more vulnerable to hackers. This summer, a vulnerability — nicknamed **Stagefright** — was found in the

open source code of the Android OS. The bug was considered a threat to 95% of Android devices — nearly 1 billion phones and tablets. This prompted Google and companies like Samsung and LG to rethink how they provide software updates.

Apple users have long enjoyed a somewhat higher level of security, thanks in part to the company's proprietary approach to software and hardware. With fewer third-party manufacturers involved, Apple has been able to lock down its systems more easily. Also, until recently, Apple didn't have much adoption in the corporate world, so hackers chose mainly to target Windows-based machines instead. But those days may be coming to an end.



A security issue has come up recently for Apple, and it's worth noting for those who use iPhones or iPads. The company announced it has discovered dozens of malware-infected apps on its popular App Store, including **WeChat**, which has more than 500 million monthly users. This is considered Apple's first major cyber attack since it shows the App Store can be compromised on a large scale. It also demonstrates that the company's popularity has made Apple's iOS — and its users — a target. The recent Apple incidents may be somewhat minor where only 39 malware-infected apps were removed from among the 1.5 million apps on the App Store but they are worth noting. Apple's security has historically been solid, but that doesn't mean you are completely protected.Because of the ability to sync smartphones to desktops and laptops, problems that start in one device can quickly spread to others. Put some protections in place so that you can enjoy your Apple and stop hackers from taking a big bite.

TABLE 1
SECURITY COMPARISON BETWEEN ANDROID AND iOS

Features	**Security Comparison in Mobile OS**	
	Android	***iOS***
Application Sandboxing	Each app has its own sandbox	All apps shared same sandbox
Data Storage Format	Have an external storage and can be accessible by unwanted code	No external storage and difficult for the unwanted code to access built in storage
Memory Randomization	Fully applied in Nougat and started since Jelly bean. No code signing technology	Fully applied in 9.0 and 10.0 releases. Added with code signing technology
Encryption	Android 5.0 and above supports full disk encryption whereas Android 7.0 and above supports file based encryption	Hardware and Firmware encryption ; Advanced Encryption Standard(AES) 256 bit crypto engine
Built-in Antivirus	Antivirus can be downloaded from the Android market. More easy for virus attack since no protection and checking is done before outside web source application been downloaded	No antivirus is required since there is checking been done in the Apps Store
App Store Distribution	Google play is the most trusted and used marketplace for android apps, but there are many other too which are used very less	App store constitutes 90% of apps distribution by iOS users but there are other too which are used very less.
App Permission	In this if you want an app , then all the permissions is to be accepted , then only you can use that app. No modification in permissions can be made by user.	Improved permission system where you can actually pick and choose which data an app gets access to. So one can modify permissions on its own
Interface	Navigation system is better and give access to its user to change according to their choice	Navigation system is restricted , allows user to put them in a folder and cannot remove the apps from home screen.
Software/Security Updates	It does not provide security update to the version lower than Android 4.4.4 that means leading to security holes for version lower than 4.4.4	It provides timely security updates for all its users
Customization	It offers far more freedom in terms of customizing the interface according to you	By contrast, it doesn't allow you to change any icons in the Control Centre
Security	There is a high chance of malwares, and virus to enter the system because it does not check for the source of download and the software or app being download	There is rare chance of malware, trojans or virus enter the system as there is no option provided to download other than app store and other trusted sources.
Fragmentation	The fragmentation is more because being an open-source as well as so many versions are there.	The fragmentation is lesser than android being a closed source and providing security-patches to all system having iOS
Vulnerabilites	There are 850 vulnerabilities in android at present	There are 1091 vulnerabilities present in iOS at present

IV. CONCLUSION

Although both Android and iOS have their flaws, Apple's iOS has still proved to be a safer bet in terms of security. Apple runs a tight ship which can feel constricting to users, but ultimately, it is to keep their users as secure as possible. Yes, hackers have started to poke holes in the iOS but they have only managed to target jail broken iPhones and a miniscule portion of apps within the App Store. Mobile security is all about trade-offs and manage the risk. It's about how developers can reduce and minimize potential risks for consumers. The mobile user should make a choice between comfort and privacy of data.
In conclusion, we agreed that iOS are more advantage compared to Android operating System in term of security based on comparison that have made. However, there are few basic security points to keep our data safe on the respective mobile device are:

- **Update your software** : Always update your Smartphone OS, irrespective of it being an Android or an iOS, whenever any application patches or OS upgrades are released.
- **Lock your device:** If the device is being used by a stranger, use a password to lock your device to avoid data theft.
- **Don't jailbreak your devices.:** Do not jail-break, root, or modify the OS files.
- **Add genuine antivirus from authorized app-store:** Install an antivirus and firewall software to detect and stop any infection.
- **Add location tracking app**: Install device-tracking applications to find the phone whenever it is lost or stolen.
- **Backup your data**: Regularly backup or synchronize your settings and other personal information to avoid the loss of data.
- **Know what you're downloading:** Try to learn about the application's reputation before installing it.
- **Manage your data**: Control the types of data that can be accessed via mobile devices to determine your exposure should a device be compromised.
- **Use Mobile Device Management software:** Use it to create an encrypted password-protected sandbox for sensitive data and enforce device-side technical policies.

Future work in this field may involve the following topics:

1. Complete security assessment of existing iOS and/or Android applications
2. Comparison of the security between jailbroken vs. non-jailbroken Android and iOS devices
3. Security assessment of the enterprise features of Android and iOS on Mobile device management, configuration profiles, and Wireless app distribution
4. Security assessment of the In App Purchase system and App Store application distribution

REFERENCES

[1] Grace, M., Zhou, J., Wang, Z., & Jiang, X. (2012). Systematic Detection of Capability Leaks in Stock Android Smartphones. In Proceedings of the19thAnnual Symposium on Network and Distributed System Security, NDSS '12
[2] K. Allix, T. F. Bissyand´e, Q. Jerome, J. Klein, R. State, and Y. Le Traon, "Large-scale machine learning-based malware detection: Confronting the "10-fold cross validation scheme" with reality," in CODASPY '14, 2014.
[3] Charlie Miller, "Mobile Attacks and Defense," IEEE Security and Privacy, vol. 9, no. 4, pp. 68-70, July/Aug. 2011, doi:1O.1109/MSP.2011.85
[4] R.Johnson, Z.Wang, C.Gagon, and A.Stavrou, " Analysis of android applications`permissions,"inProc.IEEEInt.Conf.Softw.Secur.Reliab.Companion, SERE-C, 2012, pp.45-46.
[5] Android Open Source Project, Google, "Android Developers Dashboards", 2012
[6] https://developer.android.com/training/articles/security-tips.html
[7] http://www.apple.com/ipad/business/it-center/deploymentmdm.html
2013 8th International Conference on Information Technology in Asia (CITA)
[8] "Apple - iPhone 4S - The most amazing iPhone yet." [Online]. Available: http://www.apple.com/iphone/.
[9] Prince McLean.Inside google's Android and Apple's iPhone OS as business models.roughlyDrafted Magazine.November 10,2009.
[10] Khadijah Wan Mohd Ghazali, Rosilah Hassan and Zulkarnain Md Ali, A Network Device Simulator, IEEE ICACT 2013, PyongChang Korea Jan 27-30, 2013, pp.378-381.
[11] Qing Li; Clark, G., "Mobile Security: A Look Ahead," Security & Privacy, IEEE , vol.11, no.1, pp.78,81, Jan.-Feb. 2013 doi: 10.1109/MSP.2013.15
[12] Tae Oh; Stackpole, B.; Cummins, E.; Gonzalez, C.; Ramachandran, R.; Shinyoung Lim, "Best security practices for android, blackberry, and iOS," Enabling Technologies for Smartphone and Internet of Things (ETSIoT),
[13] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," Berkeley, CA, USA, 2010, pp. 1- 7.
[14] "Symantec: Finders Will Try to Access Lost Smartphones - Security - News & Reviews - eWeek.com - eWeek Mobile." [Online].Available: http://mobile.eweek.com/c/a/Security/Symantec-Finders-WillTry-to-Access- Lost-Smartphones-350586/.