Comparison Between Android and iOS Operating System in terms of Security

Mohd Shahdi Ahmad, Nur Emyra Musa, Rathidevi Nadarajah, Rosilah Hassan and Nor Effendy Othman,
School of Computer Science,
Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia
shahdiahmad@yahoo.com, aryme_87@yahoo.com, ratz_devi_87@yahoo.com, rhassan@ieee.org and effendy@ftsm.ukm.my

***Abstract*— This paper compares between android and iPhone Operating System (iOS) mobile operating systems (MOS) that available in the market which is more specific on security issue. These issues are reportedly the concern of not only the mobile customers but also the software developers. In achieving security requirements, the MOS developers need to know how to achieve the criteria. The security requirements for MOS are Application Sandboxing, Memory Randomization, Encryption, Data Storage Format and Built-in Antivirus. Application sandboxing enforces permissions, privileges, directories, entitlements and kernel access for a mobile app. Memory randomization ensures that the memory regions of mobile application as well as system shared libraries are all randomized at device and application start-up. Encryption is performed at disk or filer/folder level and also at the interprocess communication level. It is difficult to speak in favor or against the android or iOS operating system in terms of better security. The way of using the device plays a major role in determining the security level. In term of storage, all data are stored in Data Storage Format. Data can be store at internal storage or external storage. To protect the MOS from virus attacker, antivirus need to be install for increasing security areas.**

Keywords—MOS; Android; iOS;

I. INTRODUCTION

Mobile OS also known as Mobile Operating System (MOS) whereas it use for handheld operating system. It's also known as a software platform for mobile devices which is allowed mobile devices to run application and program. This MOS combine features of a personal computer operating system and manage all hardware and optimizes the efficacy. There are several types of mobile OS in market. The two famous mobile OS nowadays are Android and iPhone Operating System (iOS). Android OS is an open source and source code release by Google under the Apache license. The operating system is a linux based and the application software running on an application framework which includes Java-compatible libraries based on Apache Harmony. This android designed primarily for touch screen mobile devices and the user interface is based on direct manipulation using touch screen. The first Android phone sold in October 2008 and latest version is jelly bean android 4.2. iOS derived from OS X that share by Darwin foundation. This IOS mainly use for apple product such as iPhone and iPad. There are 4 abstraction layers which is Core OS layer, Core Services Layer, Media Layer and Cocoa touch layer. Some of the application can be freely downloaded. For iOS application cannot directly communicate with other apps. Why we need security on MOS is to ensure all the users credential is not attacked, to make sure sensitive data is not exposed to outsider and to understand, prevent, rectify and remove viruses.

II. SECURITY REQUIREMENT FOR MOBILE OS

A. Application Sandboxing

For mobile operating system, application sandboxing have been applied to improve the security of the mobile. Application sandboxing is a container used to control and limit the application from accessing to the system or other application especially 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. 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 make 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 limits the application access to the files system, network and hardware. iOS also have a robust sandbox model where all application shared a same sandbox model which is more secured and less open to the crowd.

iOS is much better and more secured since it is only allowed user to access the system file at the root and settings of the phone not in each application. But Android relies more on user because it required user to set the security on each application during installation time.

B. *Memory Randomization*

Other security features is memory randomization or Address Space Layout Randomization (ASLR). Memory randomization is a process where the memory application, shared library and others in a device is located randomly. This is important to avoid the malicious code or virus to attack the memory of the running application. Malicious code or virus need to find the exact position or memory region of the task it wants to attack and this is complicated for them since it have been randomly locate.

For Android operating system, memory randomization is fully applied in Jelly Bean release. For iOS, memory randomization has been applied since iOS 4.3 earlier than Android operating system. It also added more secured technology where iOS have code signing technology which is a process where a digital signature is required to allow unauthorized application running in a device.

By right, iOS is more secured compared to the Android operating system because memory randomization in iOS is enhancing by the code signing technology.

C. *Encryption*

Encryption is translation of data into a secret code. Encryption is also the most effective method to archive data security. You must have access to a secret key or password that enable you decrypt a data which is in encrypted file. Unencrypted data is called as plain text and Encrypted data is called as cipher text. Encryption is important for mobile operating system because it provides 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 < 3.0. 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 to read encrypt file in Android.

Encryption is also a new security method in iOS too. Hardware encryption was introduced with IPhone 3GS. Encryptions secure all our data in Apple product. Encryption allow 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. You must have passcode to read encrypt file in iOS.

Apple iOS device protection API is more robust than Android. While designing the developers does not take advantage of the encryption method although both Android and iOS operating system supports the storage of secrets in the ciphertext mode on disks. All encrypted data can be stored in form of plain text but cannot be accessed by the developers without knowing the encryption codes.

D. *Data Storage Format*

Data storage is a place where all the data is store 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.

For Android, the storage of data can be stored in both data storage which is external and internal built in. An application in Android can access all the files throughout the device. While in the iOS, the devices itself do not have an external storage or memory. It only has a built in storage which is required permission to manipulate or access all the data. So iOS storage will be more secured than Android and make the application difficult to access the data.

E. *Built-in Antivirus*

In general there are 3 types of popular malware that affects mobile such as Virus, Spyware and Trojan. Virus is a true piece of malicious software. Virus is usually transmitted thru email. Spyware is software that collects information about users without their knowledge. Meanwhile Trojan serves a desirable function but actually the purpose of 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 vigorous vetting process. Android users can install thousands of application from Google Play safely. The antivirus features weren't actually found on Android devices but actually found in Google Play. 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 virus. 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 Android operating system. Extra antivirus solution need to be installed in Android operating system to avoid popular malware affects our mobile operating system.

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 Apps store. Apple does not allow installation from outside source. Everything thru the Apps Store is rigorously checked to make sure it does not contain malicious codes.

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.

III. CONCLUSION

Below are the comparison between iOS and android based on its security features shown in TABLE 1.

TABLE 1
COMPARISON OF SECURITY IN MOBILE OS

Features	Comparison of Security in Mobile OS	
	Android	***iOS***
Application sandboxing	Each apps have its own sandbox	All apps shared same sandbox
Memory randomization	Fully applied in Jelly Bean Release, later than iOS. No code signing technology	Already applied in 4.3 releases. Added with code signing technology
Encryption	Disk encryption	Hardware encryption
Data Storage Format	Have external storage and can be accessible by unwanted code	No external storage and difficult for the unwanted code to access built in storage
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

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:

- Always update your Smartphone OS, irrespective of it being an Android or an iOS, whenever any application patches or OS upgrades are released.
- If the device is being used by a stranger, use a Passcode to lock your device in order to avoid data leakage.
- Do not jail-break, root, or modify the OS files.
- Install an antivirus and firewall software to detect and stop any infection.
- Install device-tracking applications to find the phone whenever it is lost or stolen.
- Regularly backup or synchronize your settings and other personal information in order to avoid the loss of data due to theft.
- Try to learn about the application's reputation before installing it.

ACKNOWLEDGMENT

We would like to acknowledge this paper is a part of Computer Networking group from Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. We also would like to thanks to Prof Madya Dr Rosilah Hassan and Mr Nor Effendy which involve to accomplish this study.

REFERENCES

[1] Rosilah Hassan, Muhammad Syahrin Ab. Rahman, Mohd Rosmadi Mokhtar, Aini Aman, Mobile Accounting Version 1 Design of Mobile Costing Application for MSMEs Using Android, IEEE ICACT 2013, PyongChang Korea Jan 27-30, 2013, pp.697-701.

[2] http://www.rdacorp.com/2012/08/mobile-application-development-security/

[3] https://community.rapid7.com/community/mobilisafe/blog/2012/12/21/inside-the-sandbox

[4] http://source.android.com/tech/security/

[5] http://www.howtogeek.com/129896/htg-explains-does-your-android-phone-need-an-antivirus/

[6] https://developer.android.com/guide/topics/security/security

[7] http://www.networkworld.com/news/2012/120312-argument-ios-android

[8] 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), 2012 First IEEE Workshop on* , vol., no., pp.42,47, 18-18 June 2012

[9] 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

[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.