International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 01, Issue – 03, June – 2016, PP – 01-06

SURVEY PAPER ON ANDROID Vs. IOS

Vikas Goyal[1], Anshul Bhatheja[2], Deepak Ahuja[3]

1(Assistant Professor CSE, MIMIT/IKGPTU, INDIA)

2(CSE, MIMIT/IKGPTU, INDIA)

3(CSE, MIMIT/IKGPTU, INDIA)

Abstract: *Today the world is moving towards mobility and we think all of us have smartphones in our hands as well as in our lives. According to a survey more than two/third of the Americans own smartphones in 2013. The smartphones are also seen as replacement for the computers and laptops. The features of these smartphones are the operating system they have or the applications they support. As we all know the four major mobile operating systems present are: - iOS, Android, Windows and Blackberry. The first two owns upto 92% of the total smartphone market share. With the increase in the demand and use of the smartphones security concern is a major issue now a days.*

Keywords: *IDE, iOS, OS.*

1. Introduction

The two major smartphone market players are iOS and Android. iOS is owned and developed by Apple Inc. since 2007 whereas Android is developed by Android Inc. but now Google takes over this. Android is developed and came into existence since 2008. Our main motive to do a survey on security topic of these smartphones operating system is to make users aware about the security issues of these operating systems, what are the security threats present in these operating systems and what are the threats to user data present in these smartphones.

1.1. iOS

It is mobile operating system developed only for the Apple's Hardware. Apple does not give license to any other company or user to use their operating system on any other device. It is specially designed only for the Apple products like iPhone, iPad, iPod etc. It uses frameworks like UIToolKit, CoreFoundation and QuartzCore frameworks etc. It also uses classes like Cocoa touch and objective c classes. App Development in iOS is carried out under the Xcode IDE and objective c and swift are the languages used for the development.

1.2. App Store

It is shop for all the iOS apps whether they are free of cost or paid. All the iOS apps after successful testing by Apple are published or posted on the app store so that all other apple users can download them according to their needs. Apple takes 30 percent of all revenue generated through apps and 70 percent goes to the app publisher. Many of the apps also have in-app purchases means user have to purchase a particular feature of the app by paying some money on it.

Fig 1.1 App Store Ico

1.3. Android

Android as we all know is an open source mobile operating system developed by Google Inc. It is based on customised java classes and the IDE used in development are Android Studio or Eclipse. Likewise iOS it is not meant for some specific users any company can customize its code and can use it in their own mobile devices.

1.4. Google Play

Shop for the android apps under the direct control of Google is known as Google Play or Play Store or Google Play Store. Google after testing the apps posted them on the google play so that users can easily download it and use it in their smartphones. The apps present here are divided into various categories like productivity, games, news etc. Android apps also are free of cost and paid. Android apps also support some in-app purchases.

Fig 1.2 Google Play Icon

2. System Architecture

Here is the images which are showing the system architecture of the android and iOS operating system. Depending on these system the security of the applications and the user data is either kept confidential or can be vulnerable to the hacker attacks.

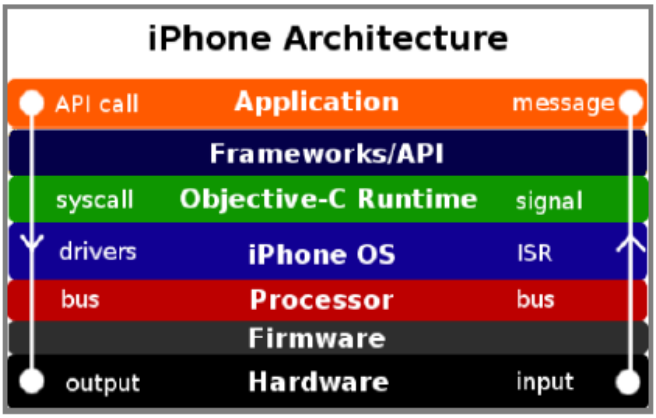

Fig 2.1 iOS Architecture

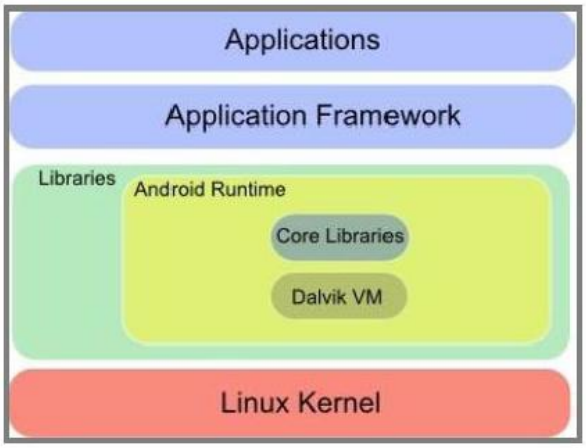

Fig 2.2 Android Architecture

3. Security at Development Time

None of the application is perfect. Some errors or bugs are caused during the designing phase of the app and some are caused due to carelessness of the developer. Due to these errors or bugs the security of the user data is compromised and the binary data injected by the attackers or hackers will be executed causing some serious threats to the user data.

In android this is the sole responsibility of the developer to isolate the application and its data from other system resources or other applications through application sandboxing. Application sandboxing in android is controlled by each application and required permission and approval to continue accessing the user data or some other things. Through this the security of any application improves and become more tighter, reliable and secure. In this application sandboxing the application has its own sandbox directory and its own app permissions.

In iOS applications sandboxing of the application is already described by the apple. Apple has set proper limits on the applications that accesses the file system, network or any other hardware. iOS also follows a sandbox model which is more secured and very less open to the crowd. iOS is much secured, better and reliable since it only allows users to access the system files through the root not from each application.

The protection of the user data stored on the smartphones is one of the most important issues that an app developer has to deal with. iOS uses encryption for both the file system as well as hardware in which files are protected using data protection API's.

4. Security at Publishing App in Store

After the development phase of an app then the developer comes to publish its app on the store whether it will be android app or iOS app. Publishing the app on the store means our application is first tested and then it is made available to the users to download and use the app. Before publishing an app on the store every app must be signed. Signing means a key is assigned to every app. This key is assigned through asymmetric encryption algorithm

5. Sandboxing of Apps in iOS

For the security reasons apple pack its each and every app (including its preferences and data) in a single sandbox at install time. A Sandbox is a set of controls that limits the application's access to the files, preferences, network resources and hardware. Through this process an app is installed in its own sandbox.

6. Sharing of Data & Apps

As we all know that android device users can share their applications, images, audio files, documents and videos with each other and to the computers and laptops also through bluetooth and sharing applications like SHAREit and xender etc. But the apple devices does not support sharing their applications, audios, images and video to any other device except apple devices (in apple devices above 5s). This is also a major feature or drawback of android devices. It is upto the user that whether they thinks this sharing among devices is a feature or a drawback of the android devices. The apple device user could download it directly from the net because apple thinks sharing of apps or any other things between devices is a major security threat to its devices as well as user data. That's why the apple makers does not provides the sharing options to its users and also the apple users doesn't ask for this feature because they also feels that apple is working very well in the field of data security. Apple is also doing well in the field of data security and the apple devices in the market really meant for offering the users high security to their confidential data and their other information. The android device makers have to work a lot on the security related to their smartphones and user data as well. So as to keep themselves in the race to compete with the apple devices and to maintain their market shares and values.

7. Technical Specification & Architecture

Table 7.1 Some Attributes of Android & iOS

Attributes	**Android**	**iOS**
Developer	Google	Apple
OS Family	Linux	OS X, Unix
Initial Release	Sep-23 2008	July-29 2007
Programmed in	C, C++, java	C, C++, objective-C

Available on	Phones And Tablets (LG, Samsung, HTC and Other)	iPod Touch, iPhone, iPad, Apple TV
Voice command	Google now	Siri
Source model	Open source	Closed, with open source components.
Latest stable Release	Android Marshmallow	9.3.2
Upcoming Release	Android N	iOS 10

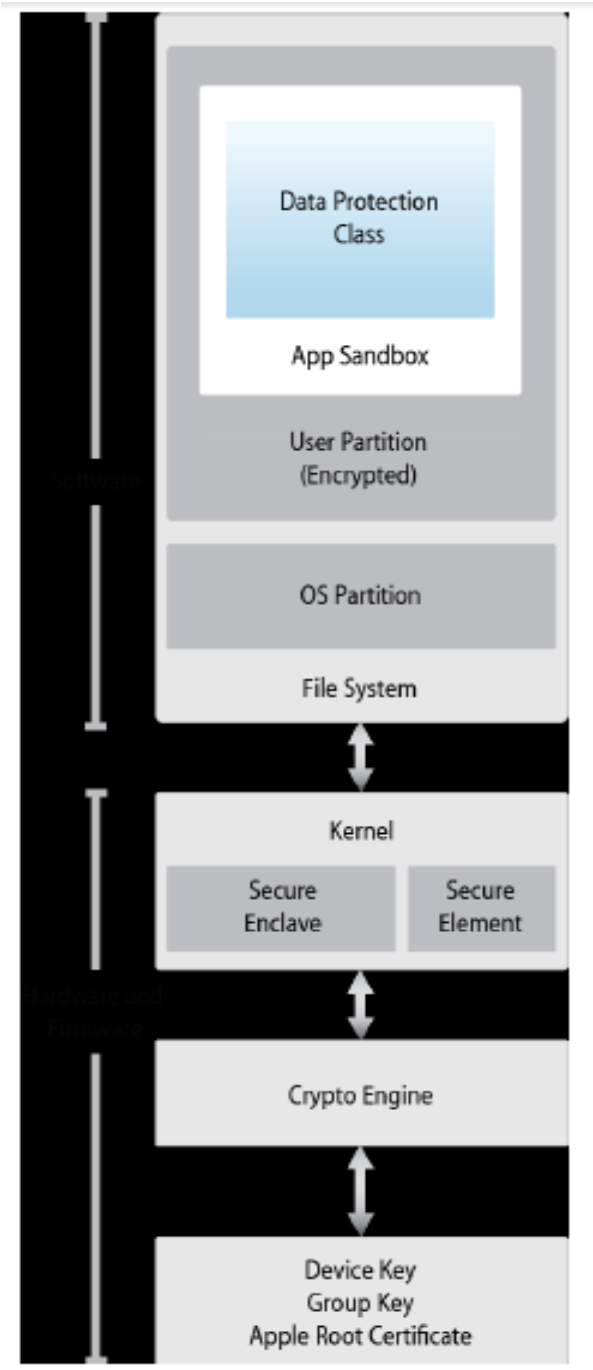

Fig 7.1 Security Architecture Diagram of iOS

Fig 7.2 Security Architecture Diagram of Andr

8. CONCLUSION

After all the study and the above discussion and the surveys, we conclude that iOS mobile operating system of Apple Inc. provide more security by supporting its Sandbox architecture for the apps. Thus providing more confidentiality to the user data. Apple is also gaining the trust of its user through these functionalities. Also the increase in market revenue of Apple Inc. is due to their devices which offer high security to the user data. Android developers and Google Inc. have a lot of work to do on it so that they can compete with apple devices.

Table 8.1 Conclusion Table

Phases	Android	iOS
Development	Application sandboxing in Android is controlled by each application and required permission and approval to continue accessing what the application needed.	In iOS application sandboxing is a set of fine-grained control that limits the application access to the file system, network and hardware. iOS has a robust sandbox model
	Each app has its own sandbox. This improves security tighter	Shares a same sandbox model which is more secure and less open to the crowd.

	Uses file system encryption only	Uses file system encryption and hardware encryption
Publish	No Code Signing.	Has code signing technology which is a process required to allow unauthorized applications running in a device.
	Account on developer console and App should have a valid certificate.	Account on App store and App must be code signed.
Installation	All types of permission are assigned to the App at installation time.	Minimal set of permission are automatically assigned during installation of App.
	User denies the permission then App installation will be aborted.	User will not be asked for any permission. No deny option is there
Execution	Seamless execution of App as no permission interruption are there	The user will be asked for permission during execution time when the App actually uses the resource
	Less secure as user will not be aware that the App may be using that resource which it is not intended for	More secure as user will be notified if any resource App want to use

9. Future Scope

In the future android device makers have to work a lot on their security related issues. They have to work hard to win the trust of the users and to increase the number of android device users. To maintain their reputation in the market different makers can come with different encryption algorithms to be used in their devices for user data security. Apple devices as discussed throughout the paper just need to maintain their security level in the devices.

References

[1]. Yogita Chittoria, Neha Aggarwal, Application Security in Android-OS VS IOS, May, 2014.
[2]. Shivam Jaiswal, Ajay Kumar, Research on Android app vs Apple app Market: Who is leading?, April, 2014.
[3]. Anuja H.Vaidya ,Sapan Naik Comprehensive Study and Technical Overview of Application Development in iOS, Android and Window Phone 8, February, 2013.
[4]. Sheikh et al, Smartphone: Android vs IOS, September-October, 2013.
[5]. https://developer.apple.com/library/mac/documentation/security/conceptual/Security_Overview/Introduction/Introduction.html#//apple_ref/doc/uid/TP30000976.
[6]. http://developer.android.com/guide/topics/security/permissions.html, June 2013.
[7]. http://developer.apple.com/library/ios/documentation/IDEs/Conceptual/AppDistributionGuide/Maintaining Certificates/MaintainingCertificates.html.
[8]. http://blog.veracode.com/2012/01/mobile-securityanhttp://blog.veracode.com/2012/01/mobile-security-android-vs-ios/droid-vs-ios.
[9]. Divya Singla, Luv Mendiratta, ANDROID VS IOS, 2014.
[10]. Wukkadada et al, Mobile Operating System: Analysis and Comparison of Android and iOS, July 2015.
[11]. Collotta et al, iOS Applications to Improve Learning and Management System in a University Campus, March 2011.

