Android vs. iOS: The Security Battle

Fattoh Al-Qershi, Muhammad Al-Qurishi, Sk Md Mizanur Rahman, and Atif Al-Amri
Department of Information Systems, College of Computer and Information Sciences
King Saud University
Riyadh, Kingdom of Saudi Arabia
(falqershi@ksu.edu.sa, mssqpr@gmail.com, mizan@ksu.edu.sa, atif@ksu.edu.sa)

Abstract **– Smartphones are one of the most demanding popular technologies in this current era of thechnology. They are comfortable for personnel use, and their adaptable functionalities give them a reputation in current competitive technology world. One of the important functionalities of these devices is to store - personal data of the users. The personal data of an user contains privacy and sensitive information which is very important. That is why now-a-days, the smartphones become primary target of a hacker. Therefore, the security technology of the smartphones becomes one of the prime research concerns within the smartphone research community. In the world of smartphones' operating systems, iOS and Android are considered the leaders. This paper focuses on those two operating systems in terms of their adopted security technologies. A review on security technologies of iOS and Android literature is presented in this research article. Furthermore, the policies and security mechanisms of the existing security models for these (iOS and Android) operating systems (OS) are discussed. Threats and malwares which target the iOS or Android are reviewed generally and specially. Two taxonomies for attacks are selected from literature and discussed for both the operating systems. Finally, the paper makes a comparison between iOS and Android based on different security criteria. The reviews result try to answer the difficult question "which OS is more secure between iOS and Android?".**

Keywords – Security; Threats; Android; iOS;

I. INTRODUCTION

The using of smartphones is indispensable activity in the nowadays daily life. The smartphones starts gradually to replace the Personal Computers (PCs) [1]. Smartphones are able to facilitate lots of services to the user like those available in the traditional PCs [20]. Moreover, there is a wide range of functionalities provided to the users by the smartphones such as personal data storing, financial transactions, governmental service's online activities, and web browsing. For these reasons and the reasons mentioned in [20], the smartphones sales achieve high number of records world wide [26]. Table 1 gives the summary of large number of shipments (in millions) of smart phones to the end users which indicates the popularity of smart is increasing day by day to the customers. The storing of sensitive personal data in the smartphones and the increasing popularity of smartphones, lead them to attract the hackers' attention. Moreover, the growing of the malware numbers is huge and is predicated to continue in growing [20,28,2,29]. These are enough motivations to make more efforts in the smartphones security.

The smartphones vendors build special Operating Systems (OSs) for their products. There are two most popular smartphones OSs in the world, iOS [23] and Android [24] developed by the two business giants namely, Apple and Google respectively. During 2011 the competition race is confined by iOS and Android across many developed countries in North America, Europe and Japan and there is a prediction to continue in the future [25].

Table 1. Canalys Report [26]. The shipments of smartphones Q3 2012, Q3 2011.

Vendor	Q3 2012 Shipments (million)	% share	Q3 2011 Shipments (million)	% share	Growth Y-O-Y
Total	**173.7**	**100%**	**120.4**	**100%**	**44.3%**
Samsung	55.5	32.0%	27.3	22.7%	103.6%
Apple	26.9	15.5%	17.1	14.2%	57.6%
Sony	8.8	5.1%	6.2	5.2%	41.1%
HTC	8.4	4.8%	13.1	10.9%	-36.1%
RIM	7.3	4.2%	11.8	9.8%	-38.4%
Others	66.9	38.5%	44.9	37.3%	48.8%
Note: shipments shown by vendor are for own-brand devices.					

Figure 1 reported by [27] shows the superiority of them among the other OSs. it also shows the race between Android and iOS. It is noticeable that Android exceeds iOS. This is related to the sharp competition between the smartphone devices who package these two OSs: Samsung devices, and others iPhone. See Table 1 again, it is clear the superiority of both Samsung and Apple. The former works with Android whereas the latter works with iOS.

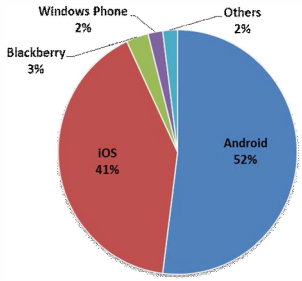

Figure 1. Nielsen Report [27] Smartphones operating system share.

Reviewing the security in terms of models, types of threats and malwares, a security multi criteria comparison between the top most smartphones Android and iOS have been introduced in this paper.

978-1-4799-3351-8/14/$31.00 ©2014 IEEE

This paper is structured as follows: Section 2 overviews the security of Andriod and iOS. Section 3 introduces the security models of them (Android and iOS) and discusses different views for each OS and the applied mechanisms in them. Section 4 reviews the threats and malwares of them. In section 5 we compare iOS against Android based on set of references and some concluded measures. We study the comparison criteria and measurements to give a sight about strengths and weaknesses for the intended OSs. Finally, discussion and conclusions are presented.

II. iOS vs. Android Security Overview

By reviewing the literature we investigate different security aspects for iOS and Android. In [8] authors developed an evaluation criteria for different OSs used in smartphones. They filled their evaluation by implementing a location tracking malicious attack. The results of their study showed that there is a very high percentage of such attack in the smartphones those are built on Android OS. Many vulnerabilities are revealed. The malicious application testing, i.e., the detection of malicious applications is not performed during the application distribution for Android OS, this is one of the major weaknesses. There is no restrictions on the source of the application (official or not market, moreover WWW or removable media, etc…). Android only executes some restrictions for the application signing and API control. The authors agreed that this offers incomplete security protection and the only strength in the Android is the remote removal mechanism. Turning over to the iOS, iPhone is considered a high secure smartphone. No unofficial market is used in iOS. The application before its uploading in the official market, it must be reviewed and signed by Apple. Also, the remote removing of suspicious application is possible with Apple. The only vulnerability mentioned is the uploading of location data to a remote server is taken place without the sense of the user.

An article [9] discussed some possible attacks and defenses for Android and iOS. About iOS the authors discussed the security advantages of Apple by mentioning it as a layered secure OS. The first layer is the using of Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) which is a technique used to distinguish the data from the code and this hardens the attacker mission. It is also noted that ASLR and DEP is used for protecting control flow attacks in windows based operating system [34]. If an attacker breaks the first layer still iOS provides a second layer, the sandboxing layer. Even for this strong security the attacks are possible. A SMS attack and a two exploit chained together attack are examples. On the other hand, for Android, the authors remarked Java as a language used for the source code and ensured its secure role in preventing memory damage attacks. They exonerated Android from the SMS attack but they confessed that the losing of DEP and ASLR in Android as a big security shortcoming. In [10] a survey on the available malwares is presented. The interested thing is that among 46 malwares, only 4 iOS attacks compared to 18 Android attacks and the remainders target other smartphones OSs. Moreover all the malwares for iOS targeted jailbroken iPhones (we will see jailbreaking in details in section 4.2). This gives indication about the number of malwares in our two OSs. The authors also stated that the permission-based, which is a main Android defense technique; need more attention by the increasing number of attacks compared to consider the iOS human reviewing as an effective mechanism against the malwares. In [33] the authors evaluated the security of different smartphones OSs in terms of messaging applications. iOS and Android approximately allow the using of all applications they evaluated. This makes them both vulnerable to set of attacks advantage from the messaging applications gaps. The authors praised iMessage tool in iOS as a defense for such attacks.

III. Security Models:

A. *iOS:*

The iOS is considered as one of the most secured OSs for smartphones. It has a strict control over its different components: hardware, OS, and applications [3]. The Apple's designers enhanced their model to reach to a model which can dispense any third party antivirus [4]. Two different views of iOS security model are presented.

The first model stands on four pillars that are mentioned in [4] and are as follows:

Device Security: Here the model interests in the saving access of the device, creating passcodes, restricting device resources, and preventing the installation of unwanted applications or using build-in services.

Data Security: The features of this dimension interest about how to protect the user data? iOS uses a 256-bit AES encryption security technique to give iOS the wiping advantage. Also it uses two others techniques: The *keychain,* which is encrypted to save both user passwords and certificates, and the *file encryption.*

Network Security: iOS provides a set of well-known protocols of network security like Secure Socket Layer Protocol v3 (SSL), Transport Layer Security v1.2 (TLS), and Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol. Those protocols enhance the security of the communications with or through the internet.

Application Security: two important mechanisms are used by iOS to ensure the application security, the *sandboxing* of the applications which is the strict isolation of the different applications, the *mandatory code signing*, and the *reviewing of the applications* in the Apple market.

The second perspective is introduced by [5]. It discussed the security as a set of different techniques to ensure the security.

ASLR: by this technique the executable code and its components such as data and links will be loaded in random memory locations. This randomization makes the memory vulnerability attacks, such as buffer overflow attacks more difficult.

Code Signing: for signing the code using trusted known certificate to give the code the authentication attribute. The signing consists from four different components.

Developer certificates where the developer of iOS apps needs to test his code into actual iOS device to see how fast it will run with different iPhone hardwares. This requires an Apple Developer Certificate. *Provisioning Profiles* which 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. *Applications Signing*, where all applications need to run in iOS, to be certificated either by Apple trusted certificates or by signing in a provision profile. *Entitlements*, it is simply a set of privileges to be coupled with the application. These entitlements are listed as keys in the XML provision profile which we just have mentioned.

Sandboxing: it is the separation between the applications which is installed in iOS. 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. This approach utilizes from the isolation of the application containers, which are the different paths of the applications installation. The iOS also adds a Sandbox kernel extension over the normal Unix-based security model to enhance the security.

Data Encryption: the sensitive data in iPhones are protected using the 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. This is also complement to what we said in the *data security* feature in the previous perspective. Other good reference is [15] and introduced the iOS security model architecture and layers.

B. Android:

Android is a famous OS and is developed by Open Handset Alliance (led by Google) [6] to be a competitive mobile OS. One of its well-known facts, is that Android is an open source OS. Both [6,7] talked about the details of Android security features. The security features are:

Application Permissions: An application permission is the allowing/disallowing a requesting of a mobile resource such as the camera, microphone or an operation.There are four permissions levels and they are as follows:*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; a 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).

Components Protection: Android OS is a component-based OS and based on the interaction between four main component types (Activity, Service, Content Provider, and Broadcast Receiver) [6]. Those components are protected from accessed by potential malicious applications. This is described as a components encapsulation by the authors in [7] and the components are classified as private and public by the authors in [6].

Signing applications: all applications in Android are archived as a package.Those packages should be signed using valid certificates. It seems that this is simple signing compared to the complicated one in iOS. There are some others security mechanisms relating to the hardware and to the programming language such as memory management unit and type safety.

Memory Management Unit (MMU): is a hardware mechanism that prevents the application processes to access memory locations of the other applications memory locations and this is used by many OSs, Android is one of them.

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.

Lastly, Android OS 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. 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. The Android is continuously updated by security mechanisms such DEP started from V2.3 and ASLR from V4.

IV. THREATS

It is expected that the smartphones will be a main target for the attackers and different types of threats. There is a huge number of threats and malwares and there is a rapid acceleration in their increasing. By viewing some reports such as [28,2,29], we could notice that. Figure 2 shows clearly the massive sudden increasing in the numbers of malwares.

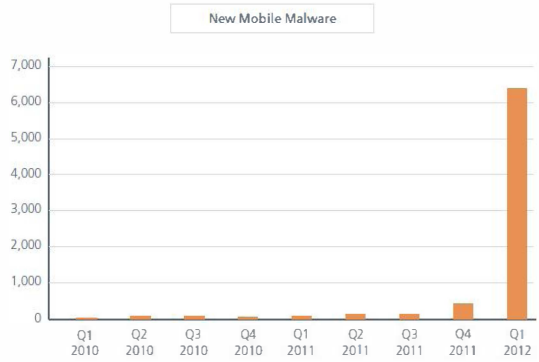

Figure 2. Total Mobile Malware Samples according to McAfee [28].

Focusing on our case, there is a set of recently reports [28,2] shown the percentage of both iOS and Android malwares. The interested notice here is the agreement of the heading of Android in the number of malwares. This is compared to all other smartphones and iOS one of them. Contradictory iOS is one of the least malwared

OSs. Figure 3 shows the percentage of mobile threats by platforms within a period of 2012. It clearly demonstrates the big difference in the percentages of iOS by 1.1% and Android by 66.8%.

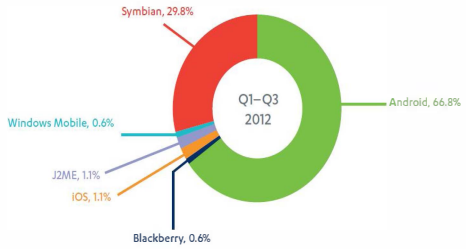

Figure 3. Mobile Threats By Platform, 2011-2012 by F-Secure [2].

Report such as [29] remarked two points, Android is the most attacked OS and comparable to iOS it is higher targeted by malewares. Other report [3] discussed some security aspects to make iOS very secure against the threats and also discussed some Android mechanisms to provide security and there is a caution said that the expectation over 120,000 malwares if the Android providers didn't update their security policies and mechanisms. A good reference reviews the malwares names and types and targets is [2]. In this report a short description for the malwares is introduced and Android malwares take the largest share.

To give an overview about the numbers of malwares for Android compared to iOS, accompanied with some names and types examples is shown in Table 2. The table shows that the Android more exposed to malwares rather than iOS.

Table 2. Malwares Comparison between iOS and Android

Ref.	*iOS*			*Android*		
	Number	**Examples**		**Number**	**Examples**	
		Name	**Type**		**Name**	**Type**
[2]	2 (0 profit motivated, 2 nonprofit)	*Fidall.A*	Riskware	42 (20 profit motivated, 22 nonprofit)	*Penetho.A*	Hack-Tool
		FinSpy.A	Trojan-Spy		*Fidall.A*	Riskware
					AdWo.A	Adaware
[10]	4	*Dutch 5Euro*	Worm	18	*Geinimi*	Trojan
		Privacy.A	Hack-Tool		*PJApps*	Trojan
					Exy (Yxe)	Worm
[20]	3	*iSAM*	Multifarious malware	1	*ZeuSMitMo*	Worm

A. *Android Threats:*

As we discussed in the previous section, Android is the most susceptible OS for threats and attacks. The authors in [30] stated three foremost explanations aspects for that: the shortage in reviewing for applications in Android official market; the openness; and the compatibility with other smartphones Apps. A set of different types of attack classes is presented in [7]. One class is a malware takes advantage of granting unaware applications permissions (permission-based) and performs its dirty roles. *Soundcomber* [11] is an example of malware takes advantages of given permission to access microphone to steal sensitive audio information and send it to a remote hacker. In [12] *PlaceRaider* is described; it is another example which uses the camera and accelerator permissions to perform a dirty stealing of sensitive data using a collection of unrealizable images. Second class hunts the points of weakness in the Linux kernel and system libraries. In [13] it is classified *Asroot* as a Linux kernel malware and *DroidDeluxe* as malware exploits an OS daemon thread. Those two malwares access the root privileges to activate their banditry. Third class malwares target the graining of the hardware of the smartphones such as CPU, and memory. Other class uses the way of the settlement in a mobile device to do attacks to other device. The SMS, MMS, and Mail attacks are effective ways for the last class. Other taxonomy for the malwares is categorized in [13]. Figure 4 briefs this taxonomy. It shows the different attack groups. First category is contains those malwares which are installed into the device. Large set of those malwares in this category using three social engineering methods. *Repacking*, which is popular one. It is the method of downloading normally the Apps and modifying dirtily those Apps and re-uploading them again to Android markets and seems like safe Apps. *Updating attack* which uses some technique of repacking but it is smarter by including only an update code to download the malicious content. *Drive-by download* attack, which is basically based on download dirty content without the users' knowledge using advertisements clicking or visiting untrusted websites. There is also other unclassified techniques such as those original Apps contain malicious procedures and those root-exploit based types.

The second main category is activation based. It is the set of threats that use the system events by registration to perform their attacks. Those events are, for instance, the booting procedure or the SMS receiving process.

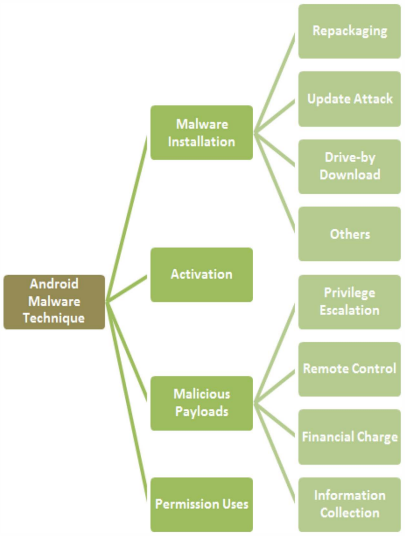

Figure 4. Android Malwares Techniques [13].

Third main group is titled as *malicious payload* group. This contains four different types of malware techniques. *Privilege escalation*, here the malwares benefit from the openness of Android and acquire a set of privileges. Famous and critical one is the root privileges set. Root exploit threats class belongs to this category. *The remote control* is other type, here the malwares use remotely the different communication tools such as http-web based and command-and-control remote server to achieve their goals. *Financial charge* is briefly the malware benefits from the premium-rate services that stolen from the

victim. Popular class is the SMS sending. Lastly in this category it is the *information collection,* here the target is the privacy of victim. The SMSs, phone contacts and other data could be stolen by the malware. The last main category is the *permission uses* and we discuss it previously as permission-based attacks in this section.

B. iOS Threats:

Compared to Android, iOS has few threats and types of attacks. The reasons of attacking Android is described in the previous section [30], and that are mitigated in iOS. There is a strict process to review and sign Apps before accepting it in Apps Store [3,4,15]. iOS is also less openness and less compatible with other third parties Apps. The literature has limited studies on iOS threats. Approximately of 200 different vulnerabilities discovered in many versions of the iOS up to April 2012[4]. One could overstate and say that the iOS users have little reasons to worry about malware [14]. In spite of that, and moreover in spite of the continuing security updates of Apple; there is no smartphone platform invulnerable from security risks and attacks [16]. One of the biggest challenges in the iOS security is the *jailbreaking* of iPhone devices. Jailbreaking described in [17] as "*a technique where a flaw in the iOS operating system is exploited to unlock the device, thereby obtaining system-level (root) access.*" As a consequence of jailbreak the root exploit is one of iOS security volatiles [14]. Jailbreak didn't take its share of literature. A brief review of jailbreaking iOS is introduced in [4]. Generally, iOS has different types of attacks and vulnerabilities. Examples of vulnerabilities are related to the iOS code signing. Others violated the data security of iOS such as the hardware and the keychain encryptions. Others, brute force ones, are about the possible decryptions of files due to the weakness of iPhone passcode which is only 4 digit .

Jailbreak is another types of vulnerabilities. All those vulnerabilities are discussed in [4].

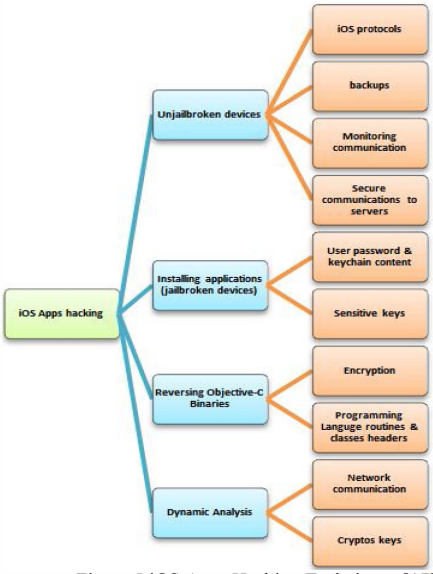

Figure 5 iOS Apps Hacking Techniques [17]

A rich description is given in [17] which gave a different practical types of attacks in iOS smartphones. As shown in Figure 5 the attacks are classified as four types. First two is caused by targeting the unjailbroken devices by installing malicious applications in jailbroken iPhones. The third class targets the objective C which is the iOS core language. Last class plays with the dynamic analysis and it has a set of opportunities for attacks and discussed in [19]. The last level contains just one attack for every type. For example, the iOS protocol attacked is *Apple File Communication (AFC)* protocol. The encryption attack is related to encrypt the iOS *Fairplay* which is a digital right management technique applied in iOS. Other study in [32] presents two types of iOS attacks which are the bootloader attacks and the browser attacks. Another one in [31] which discussed the vulnerabilities of the iOS kernel. We select some malware examples to complete the image. A survey presented in [20] contained good review for different malwares. *iSAM* is one of them and this malware introduced by [18] which is a self-propagate wireless malware connected maliciously with remote server to update its code and steal personal data. Another malware mentioned in the survey is *iKee.B* it is a child of the family of *iKee* malwares and it is analyzed by [21]. It is a botnet malware able to steal high sensitive data such as bank account information.

V. iOS AGAINST ANDROID:

In addition to the reviewing of the security of iOS and Android we build a comparison between iOS and Android OSs. This comparison is based on the security review and the threats and malwares in the previous sections which stands on the literature review, further more to some other literature perspectives.

Table 3 : Comparison between iOS VS. Android Operating Systems

Comparison Criteria		iOS	Android
Model Defense Techniques/ Mechanisms	*Code Signing*	*YES*	*YES*
	Application Permissions	*NO*	*YES*
	Sandboxing	More effective	Less effective
	Data Encryption	*YES*	*NO*
	Memory Protection	*YES* ASLR	*YES* MMU + ASLR (Android V4)
	Code Protection	*YES* DEP	*YES* Java Type Safety + DEP (Android V23)
	Availability of Antivirus tools	*YES* Few	*YES* Many
	Component Protections	Not a component based	*YES*
Vulnerabilities [8]	*Development Tools Availability*	Partial	*YES*
	Development Friendliness	*NO*	*YES*
	Installation Vectors	Restricted	Multiple
	Application Portability	*YES*	*YES*
	Unofficial Repositories	*NO*	*YES*
Strengths [8], [3]	*Application Testing*	*YES*	*NO*
	Application Remote Removal	*YES*	*YES*

	Distribution Cost	*YES*	*NO*
	API Restrictions	*NO*	*YES*
	Application Signing	*YES*	*YES*
	Keychain	*YES*	*NO*
	Authentication	*YES*	*YES*
	Device Wipe	*YES* Locally and Remotely	*YES* Remotely only
	Device Firewall	*NO*	*NO*
	Corporate Managed Email	*YES*	*NO*
	Virtualization	*YES* Virtual native OS	*YES* Virtual native Apps
	Security Certifications (FIPS 140-2)	*YES*	*YES*
Security Applications [20]	***Number***	1	6
	Examples	Lookout Mobile Security	Norton Mobile Security Lite, Kaspersky Security 9, iCareMobile
Implemented Solutions [20]	***Number***	17	24
Rating	[22] ***out of 5***	3.4	3 (Android V 3,4)
	[2] ***out of 5***	1.70 (iOS V5)	1.37 (Android V2.3)

By investigating Table 3, the criteria of building the comparison are based on a set of perspectives. We will discuss them in the following sections.

A. Model Defense Techniques and Mechanisms:

It is the smartphone OS security model defense capabilities and methods. This is discussed in the sections of iOS and Android security models. The techniques are approximately similar but:

- *With different degree of effectiveness*: the sandboxing, which iOS is more effective than Android.
- *With different tools used*: for the memory protection, the iOS uses ASLR compared to Android which uses MMU and ASLR starting from V4. Also for the code protection DEP used in iOS. However, Android uses Java Safety Type and DEP starting from V2.3.
- *With different numbers of tools*: the antivirus tools are more available for Android than iOS and this is explained by the strict restrictions of iOS Apps and the antivirus couldn't freely scan malwares.

The different mechanisms are the permissions used with Android and the data encryption used with iOS. Lastly, the Android provide components protection which is suitable for its architecture.

B. Vulnerabilities:

The comparisons under this criteria is stated by [8]. First two sub criteria, tools availability and friendliness development encourage the developers to develop new Apps. But from the security point of view those aspects are vulnerabilities because they provide more facilities for the hackers. Android provides them but iOS doesn't but only with partial availability of tools. One could conclude that, this availability and friendliness of developments explained by the large numbers of threats and malwares for Android. Second two sub criteria are the installation options and Apps market type. Those also enhance the flexibility of smartphone but violate the security. There are restricted options for installation in iOS compared to multi in Android. Also one official repository compared to one official plus many unofficial in Android. These security issues comes from facilitating the installation of malwares in the smartphones. Last point is the compatibility, which is vulnerable in both iOS and Android.

C. Strengths:

The literature in [8,3] stated a list of comparable points and we will study them in our case. One important mechanism used by iOS but not Android is the Apps reviewing. It provides protection from installing malicious malwares in the official market. They are equal by providing remotely deletion of detected malicious Apps. The cost of distribution is other security advantage hinders the attacker from adding their malwares into repository. Again this is achieved by iOS but not Android. Other measurement is the API protection and here the Android provides it. The Apps signing, the authentication, and the availability of certificates (Federal Information Processing Standard (FIPS) 140-2) are mechanisms in both iOS and Android. Firewall as a security famous tool is neither iOS nor Android built-in. The virtualization is applied in both OSs but with two different points of view. Device wipe and keychain are others security measures. Device wipe applied locally and remotely in iOS but less in Android. In Android only possible way to apply remotely. The keychain is used in iOS but not in Android. Lastly the email protection, iOS has a secure Email compared to Android.

D. Security Applications:

The security applications or what is known as antivirus applications are more available for Android than iOS and this could explained by what we mentioned about the strict restrictions of iOS applications and the openness of Android compared to iOS. This is clear, just one (Lookout Mobile Security) antivirus tool for iOS and six for Android [20].

E. Implemented Solutions:

One good thing about the development facilities, which we have criticized, is that Android has the advantage of implementing practical solutions for the different security threats. The restricted development in iOS provides less help in implementing solutions. Forty two solutions for Android are implemented against only seventeen for iOS [20].

F. Rating:

Last criteria is the referring to other scientific studies and reports to rate the security of iOS vs. Android. [22] gives 3.4 out of 5 for iOS compared to 3 for Android (V3, 4) and [2] gives 1.7 out of 5 for iOS (V5) faced by 1.37 for Android (V2.3). These ratings give a little surpass to iOS against Android.

VI. Discussion and Conclusion:

By reviewing the security aspects and existing threats for the two topmost smartphones OSs (Android vs. iOS), we try to explore strengths and weaknesses for both of them and try to make a fair comparison between them to have an idea that which one exceeds the other in temrs of different aspects of security technology.

Android attained the leadership and won the two-race in the sales over iOS. This could be explained by aspects different than the security. Android is not limited to one specific smartphone, instead it is the OS for different devices and the first in the sales (Samsung devices) runs it comparable to iOS which run with Apple devices only.

Looking for the security models of both the OS we could conclude that they use different security defenses policies beside some similar mechanisms. The iOS model is originally strict, layered, and multi-faceted security model. On the other hand, the Android model is heavily stands on the permission-based mechanism plus other mechanisms that are inherited from Android components such as Java language and its core OS i.e. Linux. iOS seems to be securer than Android but the latter tries to catch by the continuous updating.

The threats fight is considered a real challenge for Android more than iOS. The high percentage of malwares which target Android is too bigger than those hack iOS. This could be explained by the wide using of Android smartphones in the world and by the openness feature. A second reason, but makes advantage for Android, is the availability of solutions (anti-malwares products and implement solutions in the literature) compared to poor efforts in iOS.

Our comparison, based on different aspects and measures, shows the defense types, the strengths, and the weaknesses of both. Some of defenses mechanisms are applied in both and some are different for each other and this makes the security a power character in both. The vulnerabilities in Android are more than those in iOS and this is shown in the comparison. The strengths in iOS are more by a little than those in Android. Availability of solutions and anti-malwares products for Android is greater than iOS. The two ratings in the comparison are both won by iOS.

The last but not least is that, Android is the forerunner in the race of business competition but the stockholders of Android's developments should do more efforts in terms of security to continue forerunning because iOS stills a strong competitive adversary and it gives a prime focus for implementing security technology.

Acknowledgement

This work was supported by the Research Center of College of Computer and Information Sciences, King Saud University, Project No: RC131029. The authors are grateful for this support.

References

[1] Muslukhov, Ildar, et al. "Understanding Users' Requirements for Data Protection in Smartphones." Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on. IEEE, 2012.

[2] F-Secure. Mobile Threat Report Q3 2012: *http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf*

[3] TrendMicro. Enterprise Readiness of Consumer Mobile Platforms: *http://www.trendmicro.es/media/wp/ent-readiness-mobile-platforms-whitepaper-en.pdf*

[4] Symantec. Apple iOS Security in the Enterprise: *http://www.oliverkarow.de/cruft/AppleiOSSecurityintheEnterpriseWP.pdf*

[5] Trail of Bits. Apple iOS 4 Security Evaluation: *http://www.trailofbits.com/resources/ios4_security_evaluation_paper.pdf*

[6] Enck, William, Machigar Ongtang, and Patrick McDaniel. "Understanding android security." Security & Privacy, IEEE 7.1 (2009): 50-57.

[7] Shabtai, Asaf, et al. "Google android: A comprehensive security assessment." Security & Privacy, IEEE 8.2 (2010): 35-44.

[8] Mylonas, A., et al. "Smartphone security evaluation-the malware attack case." Proc. SECRYPT (2011).

[9] Miller, Charlie. "Mobile attacks and defense." Security & Privacy, IEEE 9.4 (2011): 68-70.

[10] Felt, Adrienne Porter, et al. "A survey of mobile malware in the wild." Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011.

[11] Schlegel, Roman, et al. "Soundcomber: A stealthy and context-aware sound trojan for smartphones." Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS). 2011.

[12] Templeman, Robert, et al. "PlaceRaider: Virtual Theft in Physical Spaces with Smartphones." arXiv preprint arXiv:1209.5982 (2012).

[13] Zhou, Yajin, and Xuxian Jiang. "Dissecting android malware: Characterization and evolution." Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012.

[14] Grimes, Galen A. "Are Apple's security measures sufficient to protect its mobile devices?." Wireless Telecommunications Symposium (WTS), 2012. IEEE, 2012.

[15] Apple: iOS Security May 2012: *http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf*

[16] Lookout. State of Mobile Security 2012. *https://www.lookout.com/_downloads/lookout-state-of-mobile-security-2012.pdf*

[17] RENARD, Mathieu. "Practical iOS Apps hacking." G 2 reHack 012: 14.

[18] Damopoulos, Dimitrios, Georgios Kambourakis, and Stefanos Gritzalis. "iSAM: An iPhone stealth airborne malware." Future Challenges in Security and Privacy for Academia and Industry (2011): 17-28..

[19] Szydlowski, Martin, et al. "Challenges for dynamic analysis of iOS applications." Open Problems in Network Security (2012): 65-77.

[20] La Polla, Mariantonietta, Fabio Martinelli, and Daniele Sgandurra. "A survey on security for mobile devices." (2012): 1-26.

[21] Porras, Phillip, Hassen Saidi, and Vinod Yegneswaran. "An analysis of the ikee.b iphone botnet." Security and Privacy in Mobile Information and Communication Systems (2010): 141-152.

[22] 2012 State of Mobile Security. InformationWeek reports: *http://www.ihrim.org/Pubonline/Wire/June12/2012-state-of-mobile-security.pdf.*

[23] Apple. iPhone Operating System: *http://www.apple.com/iphone/ios/*

[24] Google. Smartphone Operating System.: *http://www.android.com/*

[25] [25]comScore. 2012 Mobile Future in Focus:*http://www.theechange.ca/upload/docs/comScore2012MobileFutureinFocus.pdf*

[26] Canalys. Press release 2012/11:

http://www.canalys.com/static/press_release/2012/canalys-press-release-081112-sony-and-htc-overtake-rim-and-nokia-smart-phones.pdf.

[27] Nielsen. Nielsen Mobile Insights:

http://www.nielsen.com/us/en/top10s.html

[28] McAfee. Threats Report: First Quarter 2012:

http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q1-2012.pdf

[29] [29]PandaLaps. Quarterly Report: April-June 2012:*http://press.pandasecurity.com/wpcontent/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf*

[30] Oh, Tae, Bill Stackpole, Emily Cummins, Carlos Gonzalez, Rahul Ramachandran, and Shinyoung Lim. "Best security practices for android, blackberry, and iOS." In Enabling Technologies for Smartphone and Internet of Things (ETSIoT), 2012 First IEEE Workshop on, pp. 42-47. IEEE, 2012.

[31] Esser, Stefan. "Exploiting the iOS kernel." Black Hat USA (2011).

[32] Halbronn, Cedric, and Jean Sigwald. "iPhone security model & vulnerabilities." In Proceedings of Hack in the box sec-conference. Kuala Lumpur, Malaysia. 2010.

[33] Schrittwieser, Sebastian, et al. "Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications." Proceedings of the 19th Annual Symposium on Network and Distributed System Security. 2012.

[34] Bojinov, Hristo, et al. "Address space randomization for mobile devices." *Proceedings of the fourth ACM conference on Wireless network security*. ACM, 2011.