Volume 5, Issue 11, November 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Smartphones Platform Security a Comparison Study

Rebwar Mala Nabi
IT Department
Sulaimani Polytechnic University, Iraq

Rania A. Mohammed
Computer Network Department
Sulaimani Polytechnic University, Iraq

Rebaz Mala Nabi
Network Department
Sulaimani Polytechnic University, Iraq

Abstract- Nowadays Smart phones and other mobile devices have become incredibly important in every aspect of our life. Because they have practically offered same capabilities as desktop workstations as well as come to be powerful in terms of CPU (Central processing Unit), Storage and installing numerous applications. So, security aspect of those devices should be taken into account seriously since phone users access wide range of none secure wireless networks and download applications on free sources which may contain harmful viruses and/or malwares. The best way of securing mobile devices is to enforce good security policy through operating systems. This paper will walk around main necessary principles of security in mobile operating systems. Then will compare those principles for four main mobile operating systems such as Android from Google, BlackBerry from research motion, Windows mobile phone from Microsoft and iOS from Apple. Finally, this paper will provide some potential steps to achieve proper mobile security.

Keywords-Threats, Mobile Security, mobile platforms, security, security awareness, sensitive data and vulnerability, OS security.

I. INTRODUCTION

Currently smart phones and mobile devices have become incredibly important among people around the world. Because they have offered same capabilities as well as facilities that desktop works stations have provided. However, security aspect still is a big challenge [1]. Nowadays, the numbers of attackers and malicious programs have increased rapidly. According to threats predictions report [2]"2014 will the turning point for threats to mobile devices". Therefore, companies should provide inherent security mechanism on hands to protect user's sensitive data, the device and applications on the device as well. The best way of securing mobile devices is to enforce good security policy through operating systems So far, this paper will explore the main key criteria essential in mobile operating systems, which these attributes can make an operating system protectable and secure enough against all various attacks and malicious programs. Attributes like authentication policy, application verification and some other essential components. Then, this paper will come to make a comparison between the most popular operating systems exists in the real world such as such as Android from Google, BlackBerry from research motion, Windows mobile phone from Microsoft and iOS from Apple. In the other words, it will show how each operating system has provided or implemented the above components. Finally, this paper will conclude by giving some possible potential steps to achieve proper mobile security.

II. THE IMPORTANCE OF THIS STUDY

As we have discusses earlier that nowadays Smartphone and mobile device have become the most targetable sources for hackers and malicious program. According the threat prediction report from McAfee Labs in Q3 2014 the total number of mobile malware samples exceeded 5 million. Moreover, about 110 million Americans— equivalent to about 50% of US adults—have had their personal data exposed in some form in the past year. Consequently, it can be acknowledged that it is crucial to have the state-of-the-Art about how mobile platforms provide security mechanism. As a result, people will have right materials to choose the right platform to use daily. Finally, this survey will help platform providers to improve their security mechanism based on the finding of this study.

III. COMPONENTS OF SECURE OS

There are a numbers of essential components that can make an OS secure enough against attackers and other malicious program. Below, this paper will explore some key necessary attributes that can make an OS secure. Then, compare those attributes between the Mobile OSs mentioned earlier.

A. Authentication

By definition, authentication means how systems authorize a user, which is vital link between user's identity and the programs executed by a user. In the other words, prevent an attacker to access privacy data as well as the device which is not allowed. Now, almost all OSs have provided same mechanism for authentication. Authentication can be done by many ways. First, by something the user knows like passwords, which it has not been proved as secure method by developers since passwords can be guessed or hacked easily by using some intelligence techniques available in the computer world. Second, users can be authorised by something they possess for instance tokens and smart cards. Finally, using biometrics techniques are measured as the most secure way to authenticate a user. Hence use of personal characteristics may be harder to forge. Despite it is strengthens it has not been used by companies. The possible reason is that using biometrics will need substantial budget.

Android OS provides a password protection which means users can configure their device to ask for a password prior to access the device. The complexity of the password can be modified by the mobile administer. Blackberry OS seems provides better authentication policy. It can use Blackberry Enterprise tool to set robust policy forcing users to access their devices using strong passwords. Two factor authentications also has supported in BlackBerry OS. Moreover, secure peripherals can be added to the device such as smart cards. The company IT (Information Technology) department will be able to monitor whether security policy has been taken into account by every single user through Over-The-Air (OTA) connection [3].

With regard to windows phone, like other platforms it has provided password login which can be configured by users. In addition, windows mobile support third party authentication which create two factor authentications. Another method which windows phone can support is biometric technique for example finger print reader. ActiveSync can be used by window phone IT department to manage and set certain policies that enforce users to have password complexity rules. iPhone iOS does provide the password technique to authenticate a user. Rules and characteristics of the password complexity can be set by IT department but users have ability to override the IT policies which this can regarded as a security issues because users always tend to use simple and short length passwords. Furthermore, in iOS phone owner has permission to specify the maximum number of attempt before the device goes lock. Meanwhile, iOS has included the possibility of having two factor authentications by using secureID and CryptoCard [3]. Finally, iPhone will create a backup when phone connected to computer desktops which include all phone's data and this can be considered as weak security mechanism because when phones connect to computers they are liable for all threats and attacks.

B. ENCRYPTION

Encryption is a process of transforming plaintext to unreadable form by using cryptographic algorithms. These days, encryption has become significantly essential since all individuals and organization using their smart phones and mobile devices to manage their daily life necessaries. Therefore, nearly all companies and organizations support encryption technique to protect user's private data in or out their devices. Good intelligence [4] did a survey on how mobile phones can be managed by asking organizations whether they support encryption or not. 27% of them answered by no, while 33% are currently support encryption and the rest are planning to deploy mobile phone encryption technique. Some platforms implement partial encryption which means users can select what they want to protect. Generally, some files are not necessarily needs to be protected such as MP3, photos and etc. On the other hand, some platforms have not delivered optionality in encryption means either encrypts all data or nothing.

Google android platform 3.0 and later versions support file system encryption. Data can be encrypted using AES128 algorithm with CBC and SHA256 [5]. Key encryption can be created by using user passwords. In order to protect the key the password is combined with random salt and hashed with SHA1 [6]. .Furthermore, the password complexity rules are in placed to avoid dictionary password attacks. Blackberry provides the symmetric key encryption to protect data during transferring in/out of the device especially between BlackBerry device and the BlackBerry® Enterprise Serve. In addition, blackberry allows the selectable data to be encrypted. It can encrypt data on peripheral devices for instance memory flash cards. Another crucial service in blackberry is that allows a user to enable encryption in the way that data is either hided to a user or locked for both user and device which makes data non-movable to other devices [7].

Windows phone support variety methods of encryption such as AES, SHA1 and SHA256, HMACSHA1 and HMACSHA256 and more [8]. With regard to key encryption users do not have any ways to store their passwords in the phone instead users need to enter the password when needed. Another option to store data safely has been provided by windows phones. Users can put their data onto a secure server and access it through their phones. To guarantee security, windows phone use SSL (Socket Secure layer) to ensure data safety when user transmits data between the web and calling other web services [8]. Encryption was not supported by old iPhones iOSs until the iOS4 later version have been developed. iOS4 and later versions support hybrid encryption model. IPhone iOS uses AES-256 algorithm to encrypt all data stored memory of the device. Furthermore, email and other valuable applications can be protected by using additional layer of encryption. [5] Found that, small data will remain unencrypted during encryption which cannot be accessed by attackers unless they will have pass-code to access the phone.

C. MANAGEABILITY AND POLICY ENFORCEMENT

Platforms should be managed remotely by IT management department or developers. That would help them to implement different operation includes "monitoring, uploading, display of device characteristics, asset management, lock down and kill, re-imaging to a new device, OS software upgrades" [3]. Lack of such capability may lead to leave adverse effects on the user private data and the device itself.

Google android have delivered remote management services such as remotely wipe all data from stolen devices, lock inactive devices, provide the complexity like having letter with numbers as well as length of the password that the user creates. In order to obtain above services you will need to download device policy application from Google Apps. Android can provide updates for both security and feature related purposes. This can be done by two ways either using OTA (over-the-air) or side-loaded updates [6]. The former, can be pushed to all devices while the latter; users need to download the special zip file to their mobile phone then file has to be loaded to operating system. Blackberry can be managed remotely through BES (blackberry enterprise server). BES has consists of several windows services that implement and complete basic operation of the system. Key services are include policy service, which allows certain security controls be pushed to devices, complete new key generation and remotely lock the device when the device has lost or stolen. Policies can be sent to the devices and deployed without user knowledge or assistance. Moreover, Data logs will available for all devices which can be analysed and use this service for feature improvement in terms of application/policy modification [3].

Windows phone uses MSCMDM (Microsoft System Centre Mobile Device Manager) which is server-based software [3]. MSCMDM allows IT employers to complete certain tasks for windows mobile phones. Moreover, it allows new application be added to phone devices via wireless networks. Furthermore, data can be wiped remotely from devices whenever needed. Finally, iOS iPhone support iPhone configuration utility which is xml (Extensible Markup Language) files they contains security policy and restrictions, VPN (Virtual Private Network) configuration protocol and etc [6]. Once polices and other configurations have been installed users will not be able modify them so they have to download another update file. It can be argued that iOS provides poor strategy to remote management because the IT department has not enough control. The possible way to obtain such services user must download the update files otherwise; IT department will not have any opportunity offer any services.

D. Application Signing

Nachenberg [5] presented that digital signing is a process of ensuring whether the applications are acceptable logically as well as have the author detail for future purposes. Mobile operating system providers must have inherent mechanism to prevent installing unidentified application on their platform otherwise illegal applications may cause potential loss of user’s data. To deal with issue, nearly all platforms have same mechanism to verify applications by using code signing or testing third party applications which means each application should be recognized by relevant windows phone marketplaces. On the other words, there should be a cleverness technique to make distinction between legitimate, good application and destructive programs. That is to say, all third party application will be rejected without having appropriate signing.

Google Android OS use code signing to identify the author of application. Android market or package installer will reject any application that does not have proper signing. So every application must sign by the developer. Basically, every signed application will be placed in its application sand box which this is making all application works separately without accessing other applications. Blackberry OS has provided essential mechanism to deal with problem. It uses verifying signature of each application to guarantee that the specified application not tempered with.

Moreover, blackberry enterprise server allows IT department to prevent or allow applications by applying set of policies. Hence those applications will try to use various resources on the phone such as turning the camera on/off and afford to access user’s data on the phone as well. On the other hand, windows phone OS uses application testing and signing program to distinct between legitimate and illegal applications. Windows phone can ensure that the application is reliable and work as the user would except by testing technique. Furthermore, windows phone marketplace imposes further rules upon applications to ensure that they are acceptable socially. Distribution of application for Windows phone is only available through windows phone marketplace. iOS iPhone closely has same mechanism as declared earlier in the previous operating systems. The developer should go through the complex registering process with apple before releasing any application and then they have to obtain digital sign to release an application. There are two ways that developer can publish their application for iPhone either through application store or in corporation with Apple iOS developer enterprise program [5]. Finally, however the Jailbreak software is available which is a program that can bypass the iPhone security and allows all application be installed without having proper signing.

E. Reliability

Reliability is ability of system that can work perfectly under any circumstances and ability to recover from unexpected errors. Simply, mobile devices should not stop working unexpectedly because this may cause loss user’s work .As result company’s reputation will be affected.

Android has showed good rate of reliability according to Square Trade Research Brief [9]. The reported presented that over 50,000 smart phones only 3.7% had non-accident malfunctioning in the first 12 months. Blackberry has recorded high level of reliability because only few reports were posted by blackberry users. Square Trade has ranked the blackberry as less reliable than Android and iOS since 6.3% of blackberry phones had malfunction issue. With regard to windows phone has been considered as less reliable due the continuing crashes and freezes. However the newer version of windows phones has improved such windows phone seven which has measured even more reliable than Android according to [11]. Finally, iOS iPhone 4 was the most reliable phone due to the recording the lowest malfunction rate in one year with only 2.1% percentage.

F. Allowing Security Extensions

Allowing security extensions is significantly important since none of mobile platforms can offer adequate security mechanism for all life. Moreover, companies could have not necessary controls and policies for now and in the future. Thus companies should be able to add extensions to their platform whenever needed. This can be achieved by providing appropriate API (Application Programming Interface) or tools as well. Nearly all mobile OSs provide mechanism to allow extensions be added to with some exceptions.

As discussed previously, Google Android provides system updates and feature related purposes. This can be used to allow extensions such as updating the codes and application by using either over-the-air (OTA) or side-loaded updates.

While Blackberry can easily support future security extensions through its application programming interface (API) and other special third party applications also allows the BES access the mobile device via wireless networks. Windows Phone does support diverse extension to underlying operating system by using its API. Finally iOS iPhone has some limitation since it is using support iPhone configuration utility. Configuration utility is an xml file which allows a developer to modify or set certain updates and even provide some extension but it does allow extending security feature but users have to download from a file.

IV. STEP TO ACHIEVE MOBILE SECURITY

Due to the increasing significance of smart phone and other mobile devices to accomplish task for consumers and works, these devices become more attractive for attackers. Consequently, the security aspect needs to be deliberated very seriously. The real security can be achieved by protecting the device, user's data as well as applications on the device. Here some main essential steps to insure the mobile security:

1- Having good security awareness: educating people to operate securely such as changing their lock pin regularly, sending the errors to the IT departments whenever appeared, backing up data, and accept patched which will be provided by companies. Security awareness has become vital to achieve high level security because people are usually do not care about security and according to a survey about users attitude about privacy and security [10], roughly half of participant said either concerned or somehow concerned about mobile data security while the rest they have never thought about it. Finally, users should be learned to use latest update of software.

2- Locking the devices: Locking device is crucial part of achieving security because devices can be lost or stolen. Having lock on the devices may guarantee loss of data on the devices along with platforms should have proper policies to enforce users to have long and strong passwords. In addition, enable remote wiping.

3- Providing patches: eventually, smart phones and other devices need to be patched regularly to avoid the risks and threats which platforms may face after releasing.

4- Installing antivirus: having good antivirus will help users as well as platform to operate securely since antivirus can block bad applications and preventing malicious programs to access data and corrupt device itself.

5- Having back up of your data regularly, use encryption to hide valuable data from hackers and do not access non-secure wireless networks.

V. CONCLUSION

In conclusion, it can be identified that nearly all mobile companies have provided same security mechanism on their platforms with some exceptions. That is to say, some companies have delivered all necessary components in order to achieve better security on hands. Furthermore, smart phone industry needs more consideration in all aspect of computing especially in security area. Moreover, more security awareness will be crucial to teach how people can operate securely.

REFERENCES

[1] Jim Luo; Myong Kang; , "Application Lockbox for Mobile Device Security," *Information Technology: New Generations (ITNG), 2014 Eighth International Conference on* , vol., no., pp.336-341, 11-13 April 2014

[2] McAfee® Labs. (2014*). Threats Predictions*. Available: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2011.pdf. Last accessed 7th mar 2012.

[3] A J.Gold Associates. (February 2013). *Choosing an Enterprise-Class Wireless Operating System: A Comparison of BlackBerry, iPhone and Windows Mobile.* Available: http://us.blackberry.com/business/leading/Choosing_an_enterprise-class_wireless_operating_system.pdf. Last accessed 7th mar 2012.

[4] Alan Goode, Managing mobile security: How are we doing?, *Network Security,* Volume 2010, Issue 2, February 2010, Pages 12-15, ISSN 1353-4858, 10.1016/S1353-4858(10)70025-8. (http://www.sciencedirect.com/science/article/pii/S1353485810700258)

[5] Carey Nachenberg VP, Fellow. (2013). *A Window Into Mobile Device Security*. Available: http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jun_worldwide_mobilesecuritywp.

[6] Android website. (2014). *Android security overview*. Available: http://source.android.com/tech/security/index.html. Last accessed 28th Feb 2012

[7] Research In Motion. (13th Nov 2011). *Feature and Technical Overview*. Available: http://docs.blackberry.com/en/admin/deliverables/12935/BlackBerry_Enterprise_Server_for_MDS_Applications-Feature_and_Technical_Overview-T305802-967621-1130113534-001-4.1.7-US.pdf. Last accessed 4th Mar 2012

[8] Deb Shinder. (Jan 12, 2011). *Windows Phone 7 Security Implications.Available*: http://www.windowsecurity.com/articles/Windows-Phone-7-Security-Implications.html?printversion. Last accessed 5th Mar 2012.

[9] SquareTrade Research. (3, 2014). *Smart Phone reliability*. Available: http://www.squaretrade.com/htm/pdf/cell_phone_comparison_study_nov_10.pdf. Last accessed 8th Mar 2014.

[10] Kurkovsky, S. Syta, E., "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security," *Technology and Society (ISTAS), 2010 IEEE International Symposium on* , vol., no., pp.441-449, 7-9 June 2010 doi: 10.1109/ISTAS.2010.5514610

[11] Seth Brodeur . (2011). *Study finds WP7 hardware more reliable than Android.* Available: http://www.wpcentral.com/study-finds-wp7-hardware-more-reliable-android. Last accessed 9th Mar 2012.

BIBLIOGRAPHY

[1] Ghorbanzadeh, Parviz; Shaddeli, Aytak; Malekzadeh, Roghieh; Jahanbakhsh, Zoleikha; , "A survey of mobile database security threats and solutions for it," *Information Sciences and Interaction Sciences (ICIS), 2010 3rd International Conference on* , vol., no., pp.676-682, 23-25 June 2010 doi: 10.1109/ICICIS.2010.5534685

[2] Krishnan, P.; Hafner, S.; Zeiser, A.; , "Applying Security Assurance Techniques to a Mobile Phone Application: An Initial Approach," *Software Testing, Verification and Validation Workshops (ICSTW), 2011 IEEE Fourth International Conference on* , vol., no., pp.545-552, 21-25 March 2011 doi: 10.1109/ICSTW.2011.10

[3] Apple Inc. (2014). *iPhone Configuration Profiles.* Available: http://help.apple.com/iosdeployment-ipcu/?lang=en#appc28ee0f4. Last accessed 1th Mar 2012.