International Journal of
Applied Mathematics,
Electronics and Computers

ISSN: 2147-8228 http://ijamec.atscience.org

Advanced Technology and Science

Original Research Paper

Security Evaluation of IOS and Android

Ahmet Hayran *[1], Muratcan İğdeli[1] , Atıf Yılmaz[1], Cemal Gemci[*1]

Accepted 9th August 2016

Abstract: — In the race of smartphone operation systems, IOS and Android seem to have the big part of pie. Both platforms have grown more enterprise-friendly since about one decade. Their adaptable functionalities make people' lives easy and give them a reputation in the current competitive technology world. We all have our personal thoughts it comes to features, usability and design. However, what about security? Mobile devices, smartphone operation systems run on, hold valuable, sensitive and classified information or content. So, that increases their attractiveness as targets for cybercriminals. The security of these devices is a growing concern and focus point for smartphone users. Eventually, the security technology of the smartphones becomes one of the prime research and these smartphone vendors have increasingly focused on security in their design efforts. In this paper, factors that influence security within IOS and Android are studied to promote the discussion. Security technologies of IOS and Android are briefly presented. And, varies factors are considered such as methods of application distribution, reduced attack surface, privilege separation, permission-based access control, sandboxing, data encryption, data execution prevention and address space layout randomization, geo-location and auto-erase. Then, brief information is given about malicious apps. Lastly, discussion is concluded to answer that tight question in the light of security models investigation and evidences collected from current life.

Keywords: mobile security, mobile device, mobile OS, IOS, Android.

1. Introduction

Mobile devices are rapidly becoming the platform of choice for consumers and businesses. There is a wide range of functionalities provided to the users by the mobile devices such as fast connnection to social platforms, personal data storing, financial processes, web browsing and tons of services.Therefore, the smartphones sales acihev high number of records worldwide and going on to suppress other electronic technologies like notebboks and tablets[1]. On the other hand, while the number of mobile devices increased, the security threats such as privacy violation, malicious code and exploits in smart environment increased. According to a recent report from Gartner, global smartphone sales are estimated to reach 1.5 billion units in 2016, a 7 per cent growth from 2015 [2]. Also worldwide smartphone sales to end-users by operating system in 2014 and 2013 are shown in Table 1 [3].

Table 1. Smartphone Sales in 2014 and 2013

OS	2014 (Units)	2013 (Units)
Android	1,004,675	761,288
IOS	191,426	150,786
Windows	35,133	30,714
BlackBerry	7,911	18,606
Other OS	5,745	8,327
Total	1,244,890	969,721

As mobile platforms become increasingly popular, so do the incentives for attackers, especially when mobile payment transactions are projected to reach almost US$630 billion by 2014. Recent security surveys describe the rapidly increasing number and sophistication of mobile attacks. Mobile devices' prevalence and mobile threats' rapid growth have resulted in a shortage of mobile-security personnel [4].The storing of sensitive personal data in the smartphones and the increasing popularity of smartphones, lead them to attract the hackers' attention [5]. Cybercriminals have found many sophisticated ways to perform malicious activities on mobile devices. Cybercrimes such as identity theft, information theft, distribution of malwares, and financial fraud have become a real threat to individuals, organizations, and service providers. Nevertheless, there are defences that can be put in place to minimize and mitigate these threats [6].Although academic research in mobile device and smartphone security has been conducted for several years now, it's only recently— due to the explosion of mobile device deployment in the enterprise environment —that those research activities have truly focused on solving real-world security challenges [7].

In this study, Security technologies of IOS and Android are briefly presented and considered. Then, brief information is given about malicious apps and exploits. Lastly, discussion is concluded to answer that tight question in the light of security models investigation and evidences collected from current life.

2. Evaluation of Security Factors

In this part of study, security factors that have chosen for comparison are evaluated.

2.1. Application Distribution

App Store is the only place to distribute apps. Therefore, the apps must be uploaded that official marketplace for public. Before this process, developer must register with Apple and gets aware of license conditions. After registration, digital certificate can be

[1] *Computer Engineering Department, Baskent University, Ankara/Turkey*
**Corresponding Author: Email: ahmethayran@gmail.com*

Note: This paper has been presented at the 3rd International Conference on Advanced Technology & Sciences (ICAT'16) held in Konya (Turkey), September 01-03, 2016.

obtained to sign app for distribution. Aim of digitally signing is to guaranty that both the identity of the app's developer and the app are not modified, and that app is belongs to intended developer. Second important step to publish app is vetting process. Vetting process is process for checking application for privacy and security violations [8]. That process can be taken one or more weeks. Also, some other issues that may get developer into trouble are explored during this process. For example, the app that works with public web site in real time needs to be confirmed its own End User License Agreement (EULA) by users and web site moderator must check and decide the content that send over that app to publish or not.

For Android, users need to create account on Google Play as a publisher like Apple. But signing and vetting processes in Google Play are different! Android does not require the applications' developers to sign apps with Google-issued signing certificates. Actually, developers who want to post their apps on Google are able to create as many self-signing certificates as they want without being monitored by Google [9]. That leads to some security vulnerability such as attackers can use famous company name to fasten their malicious app distribution. Also, vetting process in android is shallow and automatic means not checked by human beings. This situation gives easy way to put malicious apps on this trusted domain play.google.com. Also, there is more important issue here Google Apps (APK Files) can be published over anonymous web site or over e-mail. That totally leaves the decision to consumers for installation. But, one central problem is the inability of users to make good security choices and awareness [7].

Some Applications

2.2. Reduced Attack Surface

The attack surface is the code that processes attacker-supplied input. If app has vulnerability in some code, and either the attacker can't reach it, an attacker cannot base an exploit on this vulnerability. Therefore, a key practice is minimizing the amount of code an attacker can access, especially remotely [10].

For example, flash has a history of security vulnerabilities and not available on IOS. Android is still going on support it. In addition, there are vulnerability occasions reported about PDF viewer on Android such as some script in PDF performs dropper functionality. But, IOS render PDF files natively, only some features of it parsed. That reduces the number of potential vulnerabilities.

Also, security problem of WebView has been studied before and still exists [11]. Interestingly, research has shown that the WebView technology can be further exploited to break the sandbox protection mechanism in the underlying mobile OS. More mobile applications that integrate WebView, the broader the attack surface will become [7]. This problem is closely pursuing by these tow big companies.

2.3. Privilege Seperation

Both IOS and Android kernel implements a privilege separation model like on UNIX system. In privilege separation model, mobile operation system requires every application run with its own group and users. Thus, this ensures that applications have no permission to access other applications. The most important system processes run as a *root* that is most important privilege. Usually, phone manufacturer use this *root* right for system apps. Applications you are downloading from store will run as *mobile*. An attacker who gets full control of the app such as the PDF viewer will be constrained by the fact the code she is executing will be running as *mobile*.

2.4. Permission-Based Access Control

Both IOS and Android kernel implements a privilege separation model like on UNIX system. In privilege separation model, mobile operation system requires every application run with its own group and users. Thus, this ensures that applications have no permission to access other applications. The most important system processes run as a *root* that is most important privilege. Usually, phone manufacturer use this *root* right for system apps. Applications you are downloading from store will run as *mobile*. An attacker who gets full control of the app such as the PDF viewer will be constrained by the fact the code she is executing will be running as *mobile*.

2.5. Sandboxing

IOS and Android sandboxing mechanism sometimes called isolation almost similar where each application is separated from other applications and system's kernel. Isolation limits a process's ability to access sensitive data or system resources from another process. Still, there is slight difference between them. In Android, each application is given permissions to access certain resources, and the isolation system prevents accessing resources beyond the approved permissions. In IOS, developer himself can't define permission mechanism. It is mean that there are certain access rules defined by IOS that takes over some responsibility from end users shoulders. IOS isolates some apps from the in-out email boxes and the SMS of a device. For instance, apps cannot send SMS without the users' involvement. Of course, apps can still access some resources on the system. Thus, an attacker can use a malicious application to steal private information such as the device's unique ID, sending email spam, or performing an off service (DoS) attack on the device [8]. In Android, some ways are also open for attackers. For example, app list can be retrieved by another app using certain permissions. And, files on SD (Secure Digital) card can be read and modified by an app without any restriction.

2.6. Data Encryption

The features of this dimension interest about how to protect the user data. In IOS, generally there are two-protection mechanisms that are hardware security and data protection. Every IOS device has a dedicated AES 256 crypto engine implemented in silicon using UID and GID as key. Integrating these keys into the silicon helps prevent them from being bypassed or accessed. The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so the files cannot be accessed if someone moves the memory chips from one device to another. In addition to the hardware encryption features built into IOS devices, Data Protection technology is used to further protect data stored in flash memory on the device. This feature use Hardware Key and Passcode Key. Data Protection is automatically enables by setting up a device passcode. In addition to unlocking the device, a passcode provides entropy for certain encryption keys. This means an attacker in possession of a device can't get access to data in specific protection classes without the passcode. Besides, IOS keychain securely store passwords and other short but sensitive bits of data, such as keys and login tokens. Keychain data is protected using a class structure similar to the one used in file Data Protection [12].

For Android, data encryption likes IOS with a few missing. Android encryption mechanism is not powerful and sophisticated as IOS. Basically, there is no hardware level encryption and for file protection it uses 128-bit AES. Also, it is hard to guarantee that the file system encryption is enabled. So, this feature selected by the user.

2.7. Data Execution Prevention and Address Space Layout Randomization

DEP (Data Execution Prevention) is the another layer for security in IOS where a processor can distinguish which parts of memory can hold executable code and which parts are data. In that, DEP just allow execution of the code not the data. That hardens attacker mission. For example, when an exploit tries to run a payload that is injected into the process, DEP prevent data from execution. There are one way to bypass DEP is to use ROP (Return-Oriented Programming). In ROP, attackers harness existing valid code in memory to perform desired actions. However, to do this, they need to know where the code segments they want to reuse are located. Address space layout randomization (ASLR) makes this difficult by randomizing the location of objects in memory. Also, writing large payloads in ROP is very time-consuming and complex. This makes exploitation of IOS more difficult than just about any other platform [10].
In Android, before version 4.0 there is not this kind of special security layer. On the other hand, Android leaned on code signing and memory management unit to restrain attackers from reaching intendant memory location. But, after version 4.0 android implemented DEP and ASLR in its system core.

2.8. Geo-Location and Auto-Erase

Geo-Location is very useful feature to locate your phone in case of lost. Apple as a feature of its operating system and accompanying online service provides this feature. Our smartphones carry with them lots of sensitive data that, in the wrong hands, is capable of being used for identity theft and fraud. For this situation, auto erase come to help. If your phone is stolen or lost you can wipe your personal sensitive data from your phone. When this feature enabled 10-failed passcode attempts will automatically erase all data on the device.
For Android, there is not native solution. But there is third party apps on market.

3. Malicious Apps

The cybercriminal motivations behind mobile malware may vary from collecting confidential data to financial gain. The three main motivations behind mobile malware include obtaining financial gain, collecting sensitive data without a user's knowledge or approval, leave a security hole in the device and accessing private networks. Also, mobile-malware functions include activity monitoring and data retrieval, system modification, and unauthorized dialling [4].
As given in evaluation of security factor, Android is the most susceptible OS for threats and attacks. The authors in [14] 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 [5]. On the contrary, in Apps Store, there is a strict process to review and sign Apps before accepting it. Also, IOS is less openness and less compatible with other third parties Apps.
Malware has significantly increased, and writers of mobile malware are targeting mostly the Android platform. The most frequently targeted mobile platform in 2013 was Android with 79%, compared to 0% threats with IOS [15]. According to McAfee, a 30% increase in the number of attacks targeting the Android operating system was detected. Moreover, out of a total of 8,000 mobile malware, Android threats make up 7,000 [16]. Of course, this statistic belongs to 2013-2014 years. As we consider the previous section, IOS and Android have been enhancing their security technology and adapting against new threats.
In sum, it can be said that most important malware attacks are related with social engineering, because user does not know what is really happening when installing new software. For this reason, Apple is making an effort to get this risky and heavy duty from user's shoulders according to Android.

4. Conclusion

The growing popularity and sophistication of mobile platforms have made security and privacy a major issue for everyone, since these devices welcome every need that a PC offers. To cope with this concern, mobile operation system vendors have been improving new techniques and technologies. Majority of these are evaluated in this study. Operation system of two giant technology providers Apple and Google are almost same in case of technology. But, in approach manner Android have a few problem. Which are signing process, permission system drawback in case of social engineering and quick vetting process. For IOS, these concerns are handled very well. Besides, App store is only place to download app.
In this study, frankly it is not tried to answer which platform is more secure. Main goal here is to open a discussion for future works.

References

[1] Canalys Report, http://www.canalys.com/ newsroom/mobile-device-market-reach-26-billion-units-2016, 2013.

[2] Gartner Report Press Release, http://www. gartner.com/newsroom/id/3270418, 2016.

[3] Gartner Report Press Release, http://www. gartner.com/newsroom/id/2996817, 2015.

[4] Bhattacharya P., Yang L., Guo M., Qian K. and Yang M., Learning Mobile Security with Labware, IEEE Security & Privacy, vol. 12, no. 1, 2014, pp. 69-72.

[5] Al-Qershi F., Al-Qurishi M., Md Mizanur Rahman S. and Al-Amri A., Android vs. iOS: The security battle, Computer Applications and Information Systems (WCCAIS), 2014 World Congress on, Hammamet, 2014, pp. 1-8.

[6] Mohamed I. and Patel D., Android vs. IOS Security: A Comparative Study, Information Technology - New Generations (ITNG),), 2015 12th International Conference on, Las Vegas, NV, 2015, pp. 725-730.

[7] Li Q. and Clark G., Mobile Security: A Look Ahead, in IEEE Security & Privacy, vol. 11, no. 1, 2013, pp. 78-81.

[8] Nachenberg C., A window into mobile device security, Symantec Security Response, Symantec, 2011, pp.4-9.

[9] Kazmi Z., Toni F., Vila J. A. and Marcos M. M., TASAM-Towards the Smart Devices App-Stores Applications Security Management Related Best Practices, in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, IEEE, 2012, pp. 1-5.

[10] Miller C., Blazakis D., DaiZovi D., Esser S. , Lozzo V. and Weinmann R., iOS Hacker's Handbook, John Wiley & Sons, 2012.

[11] Luo T. , Jin X., Ananthanarayanan A. and Du W., Touchjacking Attacks on Web in Android, iOS, and Windows Phone?, Syracuse University, Syracuse NY, USA, 2012.

[12] IOS Security in Apple Docs, https://www.apple.com/business/docs/iOS_Security_Guide.pdf, 2016.

[13] Penning N., Hoffman M., Nikolai J. and Wang Y., Mobile malware security challenges and cloud-based detection, Collaboration Technologies and Systems (CTS), 2014 International Conference on, Minneapolis, MN, 2014, pp. 181-188.

[14] Oh, Tae, Stackpole B., Cummins E., Gonzalez C., Ramachandran R. and Lim S., Best security practices for android, blackberry, and iOS, In Enabling Technologies for Smartphone and Internet of Things (ETSloT), 2012 First IEEE Workshop on, IEEE, 2012, pp. 42-47.

[15] Internet security threat report 2014, Symantec, http://www.symantec.com/content/en/us/ enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, 2014.

[16] McAfee 3rd Quarter 2013 Threat Report, McAfee, http://malwarelist.net/2013/11/20/mcafee-3rd-quarter-threat-report- released/, 2013.