Comparative Study of Security Measures in Android and iOS

Aditya S Sreerama[1], Dr. B. M. Sagar[2]

[1]B.E Student, [2]Head of Department
[1,2]Dept. of Information Science and Engineering, RV College of Engineering®, Bangalore, Karnataka, India

---***---

Abstract - *Smartphones are among the most demanding popular technologies in today's technological era. They are comfortable for the use of personnel, and their adaptable functionalities give them a reputation in the competitive world of current technology. One of those devices' essential functionalities is to store-consumer personal data. A user's personal data includes anonymity and private details and is quite significant. That's why smartphones are becoming a hacker's main focus now-a-days. Therefore, the mobile protection infrastructure is one of the key research issues within the research community. In the world of operating systems for smartphones, iOS and Android are seen as the leaders. This paper focuses on those two operating systems in terms of the security technologies they adopt. A review of iOS and Android literature on security technologies is presented in this research article. The paper takes suitable examples to assess the strengths of the method used by the two operating systems. Finally, we conclude the paper by inferring which operating system is more secure.*

Key Words: iOS; Android; Security; Mobile Technology

1. INTRODUCTION

In today's world, usage of smartphones is an indispensable activity that is slowly starting to replace the Personal Computer as they get smarter and more powerful. In addition to this, smartphones offer some user experiences and features which are superior to that offered by personal computers. Some of these are data sharing capability, financial payment services, e- government services to name a few. The storing of confidential personal data in smartphones and the increasing prevalence of smartphones is a making smartphone an attractive target for malicious hackers. In fact, there is a constant rise in malware and is expected to continue to grow. This should be enough incentive to pour more work into the protection of smartphones. Smartphone manufacturers develop their goods with different Operating Systems. Two of the most popular operating systems in the world are Android (72.6% market share) and iOS (26.72% market share) developed by Technology giants Google and Apple. In this paper, a security comparison with the most relevant Android and iOS smartphones is introduced to evaluate protection in terms of versions, styles of attacks, and malwares.

2. SECURITY OVERVIEW

We examine different security aspects for iOS and Android by reviewing the literature. In [1] the writers established assessment standards for various OSs used in smartphones. They leverage a malicious location tracking attack to complete their assessment. Results of their research showed that the smartphones that are built on Android OS have a very high percentage of such attacks. Many vulnerabilities were identified in the Android OS. It was noted that Android does not perform security checks in terms of malicious application detection and source of the application. Application could be installed from unverified sources such as the web or other third-party marketplaces. On the other Hand, iOS does not allow the installation of any unverified applications from the web or other marketplaces. Every application available on the Apple App Store is reviewed by Apple for suspicious activity. This makes iOS far more secure than Android. However, one vulnerability found was that location data was uploaded to the online server without explicitly mentioning it to the user.

In [2] the authors address a variety of potential iOS and Android attacks and defenses. The authors described iOS as a layered secure operating system. They said that layer one includes a Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) which are techniques used to separate data from the program code. The second layer that the authors noted was a sandbox layer which creates a separate address space for every application using memory. This prevent harmful applications from negatively affecting a system. They expressed that, even with these security measures hackers could attack the system with SMS Attacks and Chained Attacks. Moving on to Android, the authors absolve the operating system of the SMS attach but say that the absence of the Data Execution Prevention and Address Space Layout Randomization Layers was a big shortcoming. They say that the usage of Java as the primary language of code in android protects is from memory damage attacks.

In [3] the writers aggregate the malwares presently being used to exploit mobile technology. Interestingly it was noted that iOS had only 4 malwares, android had 18 while the rest targeted other operating Systems. Further it was seen that most of the iOS targeted malwares were aimed at jailbroken systems, which removes software and security restrictions giving users root access allowing the installation of modified, pirated applications from third party marketplaces.

3. iOS SECURITY

iOS is one of the safest mobile operating systems for smartphones. It controls its various components very strictly. Below we present some of the important security features of iOS, some of which we have discussed in the previous section.

3.1 Data Security

This deals with the protection of a user's personal data. Apple uses 256-bit AES Encryption by default which is a leap is the right direction. Apple provides a fantastic feature called the keychain which is a sensitive data management system which stores passwords and certificates.

3.2 Device Security

This deals with the control of access to the device which include local authentication such as Passcodes, TouchID, FaceID and other access control measures such as restricting access to device resources and blocking installation of unverified third-party applications.

3.2 Application Security

Application Security is provided two very important mechanisms:

1. **Sandboxing**
   It can be described as the separate working areas of different applications. This is very important since applications are created by third parties and can have malicious intent to the user and even other applications. Sandboxing isolates applications by leveraging distinct address spaces for installations. iOS extends the UNIX sandboxing protocol to enhance security.

2. **Mandatory Code Signing**
   Code Signing is the process of digitally signing program code by the software author. It guarantees the source as well as the content of the code being distributed. Code Signing along with Apple's Application reviewing process adds a strong layer of application security.

3.2 Address Space Layout Randomization

This technique writes executable code in random locations in the random-access memory (RAM). This makes buffer overflow attacks much harder to take place.

4. ANDROID SECURITY

Android is the world's most popular mobile operating system created and distributed by Google. Android is an open source operating system which is highly customizable for a variety of applications other than smartphones. Below we present some of the important security features of android.

4.1 Application Permission

Android uses the concept of asking the user to choose what resources an application gets to use. There are four levels of permissions which are dealt with in depth in [4] and [5]:

1. **Normal**: This is considered as an application Level Permission
2. **Dangerous**: This permission deals with the usage of sensitive user data.
3. **Signature**: This permission may only be granted to other packages which are signed with the same signature
4. **Signature or System**: This is a specific type of permission used to control and manipulate legacy permissions.

4.2 Component Protection

The android system is based on 4 main components:

1. Activity
2. Services
3. Content Provider
4. Broadcast Receiver

These components are protected individually by the system [4] and categorized as public and private components.

4.3 Code Signing

Android applications are compressed into packages that are to be digitally signed using certificates. This is a simple codesign unlike the complex systematic code signing seen in Ios

4.4 Memory Management Unit

This is a form of sandboxing where one application cannot address memory location of another application. In other words, the application installations are isolated.

4.5 Type Safety

Android is built on the Linux Kernal. It uses type safe programming language such as java to prevent memory buffer attacks.

5. DISCUSSION

In Analyzing security issues and risks to the world's most popular mobile operating systems, Android and iOS, we aim to examine their strengths and vulnerabilities and seek to evaluate them reasonably in order to get an understanding of which operating system has evolved better security technologies. On the business front, Android is the clear winner in terms of market penetration. However, this cannot be attributed to the security aspects of the operating system. Android is an open source project with applications ranging far beyond smartphones. Coming to the Security perspective, iOS and Android use different defense mechanisms although some of them are similar. The iOS model is rigid, layered and multi- faceted while android is heavily based on permissions and other security measures which are inherited from its building components which are Java's Type safety and Linux's safety and privacy measures. iOS is a clear winner when it comes to security, but android's constant security updates try to catch up. Another reason iOS is considered safer is because of the malwares developed for android are for greater in number, this can be attributed to the open source system and its popularity. Even technically speaking, the number of vulnerabilities in

Android is also greater. However, to combat this, the Android system has a lot more options when it comes to anti-malware software while iOS has very few.

6. CONCLUSION

Given our discussions above, android can be seen as the forerunner in terms of market share, but android stake holders will have to invest more on security measures to remain as the mobile operating system pioneer. Presently iOS takes the competitive edge on the security front.

7. ACKNOWLEDGMENT

This study was supported as a part of the Technical Seminar in the Bachelor of Information Science and Engineering Program in RV College of Engineering®, Bangalore - 560059.

REFERENCES

[1] A. Mylonas, S. Dritsas, B. Tsoumas, and D. Gritzalis, "Smartphone security evaluation the malware attack case," in Proceedings of the international conference on security and cryptography, 2011, pp. 25–36.

[2] C. Miller, "Mobile attacks and defense," IEEE Security & Privacy, vol. 9, no. 4, pp. 68–70, 2011.

[3] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in Proceedings of the 1st acm workshop on security and privacy in smartphones and mobile devices, 2011, pp. 3–14.

[4] W. Enck, M. Ongtang, and P. McDaniel, "Understanding android security," IEEE security & privacy, vol. 7, no. 1, pp. 50–57, 2009.

[5] [5] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google android: A comprehensive security assessment," IEEE Security & Privacy, vol. 8, no. 2, pp. 35–44, 2010.

[6] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding users' requirements for data protec- tion in smartphones," in 2012 ieee 28th international conference on data engineering workshops, 2012, pp. 228–235.

[7] G. A. Grimes, "Are apple's security measures sufficient to protect its mobile devices?" in Wireless telecommunications symposium 2012, 2012, pp. 1–7.

[8] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in 2012 ieee symposium on security and privacy, 2012, pp. 95–109.

[9] "All the info about your cybersecurity," Panda Security Mediacenter. Jun-2020.