Conference Proceeding Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Android Security Issues: A Review

Katoka Asumi
Student, M.Sc. Computer Science, Indian Academy Degree College, Bangalore-India

Abstract: Android is a mobile operating system developed by Google. It is based on a modified version of the Linux kernel and other open source software, and is designed primarily for touchscreen mobile devices such as smartphone and tablets. In addition, Variants of Android are also used on game consoles, digital cameras, PCs and other electronics. Several Android security issues do exist, especially when it comes to Android app security, centralized management and the ability to protect data on lost or stolen devices. The lack of control over apps is probably the most serious of the Android security issues facing enterprises. The Android Market attempts to offer some level of control over the apps available to users, but other apps some potentially harmful are available in alternative app stores or even on developers' websites. This paper discusses on potential Android security issues around apps.

Keywords: *Android, Security Issues*

I. INTRODUCTION

Android is a popular computing platform based on the Linux operating system.The operating system has developed a lot in last 15 years starting from black and white phones to recent smart phones or mini computers.The android is software that was founded in Palo Alto of California in 2003.The android is a powerful operating system and it supports large number of applications in Smartphones. These applications are more comfortable and advanced for the users. The hardware that supports android software is based on ARM architecture platform. The android is an open source operating system means that it's free and any one can use it. The android has got millions of apps available that can help you managing your life one or other way and it is available low cost in market at that reason android is very popular.The android development supports with the full java programming language. Even other packages that are API and JSE are not supported.

II. REVIEW OF LITERATURE

KarthickS et al.,[7],discuses about the misuse of app permissions using Shared User ID, how twofactor authentications fail due to inappropriate and improper usage of app permissions using spyware, data theft in Android applications, security breaches or attacks in Android and analysis of Android, iOS and Windows operating system regarding its security. He discusses about the android permissions namely normal permission and dangerous permission and how users grant the permission. He proposes than an explicit notification should be sent to the user when the shared User Id app tries to access the permissions with other apps and also display the resources used by shared User Id apps by the security tool app.

Kavitha.K et al.,[5],proposes that a proper authentication is provided to the user as the main criteria to protect the user from unauthorized access and also when downloading the application, the user has to check the EULA of a particular app. After verification the user can install the app depending on the permission the app asks from the user. They also use "centralized algorithm" to minimize the risk permission. The permission induced risk in application, and the fundamentals of the android security architecture are explored, and it also focuses on the security ranking algorithms that are unique to specific applications. Hence, they propose the system providing the detection of malware analysis based on permission and steps to mitigate from accessing unwanted permission (limits the permission). It is also designed to reduce the probability of vulnerable attacks.

A.Ayyasamy[4], presents an open source approach for creating an android application with thinking of some as specialized security issues.The manifest.xml file is the basic file which contains all the necessary permissions from the android mobile phone and request the user to accept it and how the malicious application will steal the user's data and upload it to the malware server. The information may include; International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity(IMSI) number, GPS location, GSM phone number, SDK version information, Android device model, and other resource information.

Paul Pocatilu[3],discusses about the vulnerabilities of mobile applications. The Android applications and devices are analyzed through the security perspective. The usage of restricted API is also presented.Healso focuses on how users can prevent these malicious attacks and propose some prevention measures, including the architecture of a mobile security system for Android devices. He proposes that the application should be installed from the trusted sources and based on other users reviews and scores. He also proposes to encrypt the user sensitive data using specialized application or using their own applications.

Suhas Holla et al,.[1],discusses a layered approach for android application development where it can develop application which downloads data from the server. Also, an Android Application Sandbox (AASandbox) which is able to perform both static and dynamic analysis on Android programs to automatically detect suspicious applications.They also analyses about the static and dynamic analysis of android application.Static analysis involves decompilation, decryption, pattern matching and system callanalysis. In all these cases software is not being executed. Here, a common approach is filtering binaries by malicious patterns, called signatures. Dynamic analysis which involves running the system in controlled environment and monitoring its behavior. It involves monitoring file changes, network activity, processes and threads etc. A common approach to dynamic software analysis is Sandboxing.

P.D. Meshram et al.,[2], discusses about the android database vulnerability.It focuses on the possibilities and risks of malicious apps leaking information by means of illegitimate approaches. As the compiled byte-code file, classes.dex keeps the information that attackers need in order to write queries through client apps, attackers need to restore source programs through reverse engineering.

Shahid Iqbal et al,.[6],discuses about the Shared User ID permission misuse following twofactor authentication failure etc.The security has been based on permission basis. Developers provide the permission and the users are given the

option to whether accept or decline the permission. Since the android is an open source software anybody can develop and built an application and can overlook the security for an application which makes it hard to secure the application from various attacks. The root cause for application's permission misuse in Android is Shared-user ID. Users do not know which app is draining their critical data using permission loop hole, there for, in the proposed methodology, a security tool, which is Android based, is developed.

Bahman Rashidi et al.,[8], discuses about the existing android security threats and existing security enforcement solutions and also reviews the strength and weak points of the solution.

CONCLUSION

Along with the increasing prevalence of Android smartphones, the number of Android apps including malware is increasing daily. In spite of deployed Android security mechanisms, malware take advantage of the Android security holes to misuse the granted resources. Thereby, many efforts have been proposed to restrict the outreach of vulnerabilities in Android devices.

References

[1] Suhas Holla, Mahima M Katti "Android Based Mobile Application Development and its Security" International Journal of Computer Trends and Technology- volume3Issue3- 2012

[2] P.D. Meshram, Dr. R.C Thool "Vulnerabilities in Android OS and Security of Android Devices" 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN)

[3] Paul Pocatilu "Android Application Security" Informatica Economica, vol. 15, no.3/2011

[4] A. Ayyasamy "Survey on Android Application Advancement and Security" 2015 Seventh International Conference on Advanced Computing(ICoAC)

[5] Kavitha K, Salini.P, Ilamathy.V "Exploring the Malicious Android Application and Reducing Risk Using Static Analysis" International Conference on Electrical, Electronics, and Optimization Techniques(ICEEOT)-2016

[6] Shahid Iqbal, Amber Yasin, Talha Naqash "Android (Nougats) Security Issues and Solutions" Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)

[7] Karthick S, Dr. Sumitra Binu "Android Security Issues and Solutions" International Conference on Innovative Mechanisms for Industry Applications(ICIMIA 2017)

[8] Bahman Rashidi, Carol Fung "A Survey of Android Security Threats and Defenses" Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 6, number: 3, pp. 3-35.