IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEW OF ANDROID OPERATING SYSTEM SECURITY ISSUES

Authors :-

I. **Mayuri Bapat**
II. **Kunal Dilip Bhagat**
III. **Adinath Navnath Ghule**
IV. **Anurag Santosh Kharade**

ABSTRACT :-

With the growth and development of mobile phone operating systems and hardware technology, security issues have become a major challenge. Currently, Android occupies a large portion of th e smartphone operating system market. As the power and capabilities of these phones increase, their security vulnerabilities also increase, making them vulnerable to threats. A permission mod el used by the Android operating system that allows Android applications to access smartphone i nformation, device information, user data, and external resources. On Android, app developers must declare permissions. In order to run the Android application, users must accept certain per missions. These permissions are verbal. If the user gives permission, the application can access data and resources at any time during installation. Again,not need to ask for permission. Androi d operating system is vulnerable to various security attacks and vulnerabilities due to its weak se curity. In this review, the author conducts aresearch on why the security of the Android operating system is so important, showing some of the needs of the Android operating system, as well as its security attacks and problems. Security measures are now in place to ensure security and ensure solutions are available.

INTRODUCTION:-

There are many types of mobile operating systems on the market. Android is one of the mobile operating systems that runs on the Linux kernel. Android operating system is open source and its source code is released under the Apache license. This code is used to control mobile devices by google supported Java Android mobile applications built based on the Java library It is the main platform used to develop mobile applications using the software suite provided by Google.Platform security is better for Blackberry or J2ME.platforms. In general, programs cannot write or read each other's code. Android SDK. Android, with its Java language and class libraries, pro

vides Unix users with useful features such as shared memory, preemptive multitasking identifiers (UIDs), and file permissions. In the first quarter of 2016, Android's market share was 84.1%, while iOS, BlackBerry, Windows and others were14.8%, 0.2%, 0.7% and 0.2% respectively. Android is one of the most popular smartphone operating systems in the third quarter of 2016.
There are 2.6 million applications in the Google Play Store.
With a total of 2.1 billion smartphones based on the Android operating system sold, Android clearly has the largest market share compared to other mobile platforms. Apple created iOS (iPhone OS), which is only available on Apple devices such as iPhone, iPod and iPad touch. iOS is the most popular operating system after Android. You installed software from an unknown source. In addition to the Google Play Store, Android users have a few other options. However, on iOS, these apps can only be installed from the AppStore. It is one of the biggest security problems in Android. Because there are many security vulnerabilities. Several steps have been taken to resolve security related issues in the Android operating system and understand the current status of these issues.

I.SECURITY AND SECURITY ISSUES IN ANDROID :-

The security of the Android operating system is based on permission-based control and control of access to critical resources by third party applications on Android. For developers, end users, and marketers, this licensing technology is often criticized for poor license management and auditing. Users can accept or reject all permission requests when installing the app. It is easy for Android OS users to have their information leaked, putting themselves at risk. Here, the main security attacks and problems of the Android operating system will be discussed.[12]

A. Spyware

Spyware is one of the main causes of serious security problems in the Android operating system. Spyware is a type of malware. When a user installs a program from an unknown source and visits a malicious website, the apk file will be downloaded immediately. You can install programs on Android from anonymous sources as well as the Google Play Store.[5]

B. Plausible Attacks

Obviously, critical resources can be accessed without seeking proper authorization. It causes malicious programs to cooperate with other programs. [6]

C. Information Leakage

Information leakage occurs when a user provides resources without limitingperformance. However, the Android operating system's permission control cannot protect users' privacy and resources from malware. Leakage of sensitive information puts equipment in a critical situation. This vulnerabilityis very easy to exploit because an attacker can access parts of the device that store sensitive data. Leaked Android apps may store sensitive user information in an unsecured location on the device or send device-identifying information (such as app metadata such as network content) to third parties. Providing user information in unsecured areas of the device may result in the transmission of device-identifying information, such as application metadata, as well as network content. Other malicious programs on the same device can access unsecured areas of the device. The impact of Android device data leak is huge. According to the Information Security Agency's website, 58% of Android devices contain private data and about 3% leak PII (Personally Identifiable Information). [19]

D. Crashes

From the user's perspective, the danger of crashes is real. The user uses the same certificate to install applications and provide various permissions that may or may not be important. Once installed, these applications can use a shared UID to access all their resources and permissions.[10]

E. Denial of Service Attacks

Excessive use of limited CPU, memory, battery power and networkbandwidth is the main target of DoS attacks. The number of mobile deviceconnecting to the Internet as a large network continues to increase, which could be a step in the development of DoS attacks. Since smartphones have less or no better protection than PCs, creators of malicious applications see them as a suitable platform for DoS attacks.

F. Repackaging Practices

Repackaging is one of the biggest security issues in the Android operating system. On the Android platform, repackaging technology can hide dangerous code, just like traditional applications. Since the repackaged applicationworks the same as the original application, it is difficult to distinguish the malicious program from the valid program. Repackaging is a disassembly/decompilation process that uses reverse engineering techniques to kill the .apk file and insert (inject) malicious code into the main code.

Repackaging:

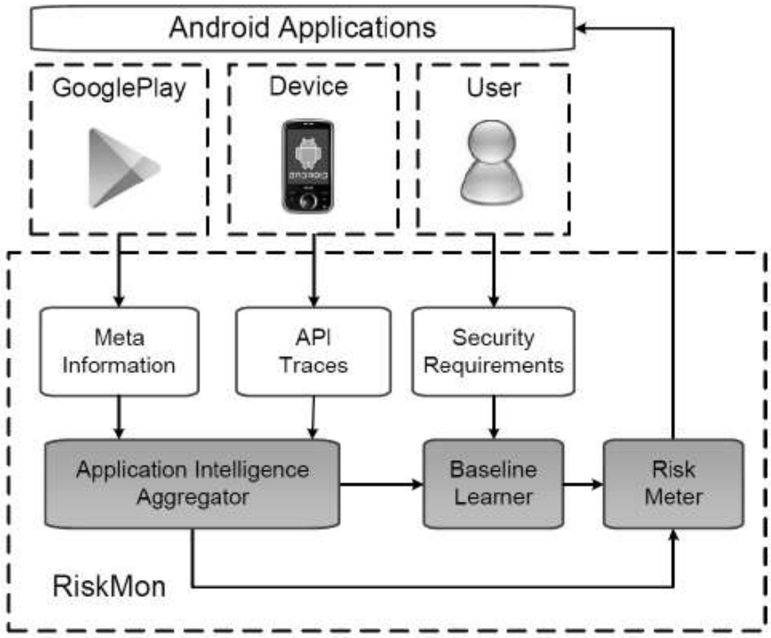
Use apktool to create files and use jar signer to sign repackaged files.
Geimini and KungFu Trojans are examples of APK repackaged Trojans.
Many legitimate Android applications may contain these Trojans.

II. Solutions/analysis :-

Some security solutions have been proposed in the Android operating system and this section is divided into two groups. They are dynamic and static and can be used for vulnerability analysis, assessment , and discovery. The dynamic method takes a lot of time and is especially necessary in cases where the application is not open. The static approach is fast but needs to be managed negatively. Hybrid methods also exist that combine the limitations of static and dynamic methods.[17]

A. RiskMon

Author requested RiskMon. Creates a risk assessment that includes appropriate behavior by linking operational and user expectations to application reliability. Figure 1 shows the basic architecture of RiskMon.RiskMon is a machine learning solution that solves this problem and provides the basis for continuous and automated risk assessment.Applications are an important part of the user framework.See. First, it records user expectations regarding applications installed on the device and evaluates the impact of group permissions on those applications.Based on data then collected from users
Forms the basis for risk assessment of IT use.
Finally, RiskMon ranks applications by interaction risk, which is measured as a variable in risk assessment.RiskMon is used without solving the interaction problem using Binder and the third equation. This indicates potential attack vectors that could bypass RiskMon.[16]



B. Kirin

Author asked Kirin to perform security procedures before implementation, improper authorization practices, and request permission to find signatures. The main purpose of Kirin is to prevent the installation of malicious applications by using certificates for applications. Here, rules are interpreted as authorizations that are difficult, leading to abuse of authority and poor performance.
Using this system during installation can help business owners instantly decide whether to install an application.
Top Ranked Apps from the Official Android App Market
They tested Kirin using 311 downloads apps. Qilin
Detected 5 malicious apps with high security after testing. Figure 2 shows the Kirinbased component and its software installer flow. They use a static scanning tool called Pscout to extract all special permissions of an Android app without modifying the app.[2]

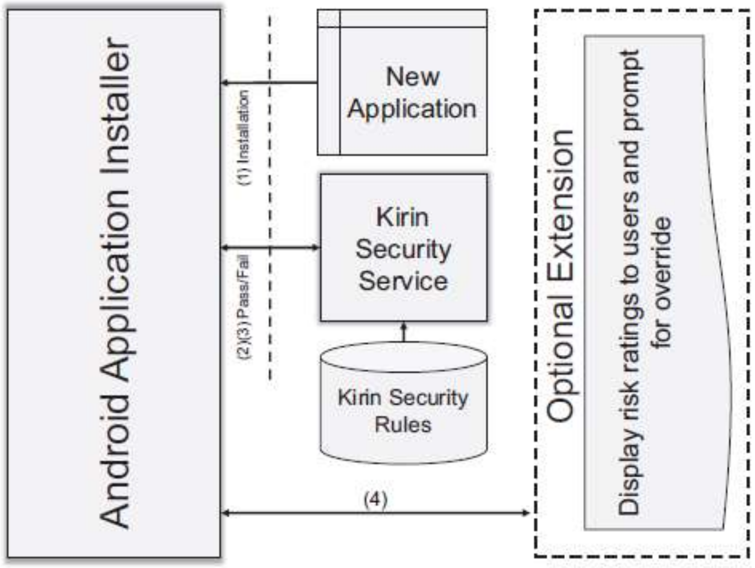
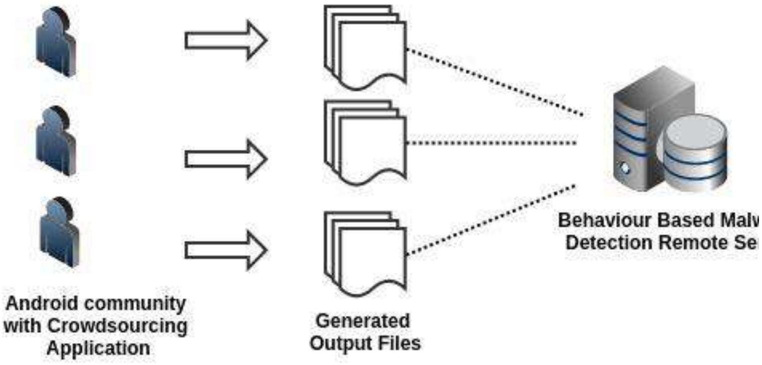


Figure 2: Kirin-based software installation process and components

C. Crowdro

Author proposed a framework for analyzing Android application behavior that can be used to identify applications with similar names and different models but different behavior. The crowdsourcing framework checks for misbehaving apps. Crowdroid is a behavior-based malware detection engine. [4]

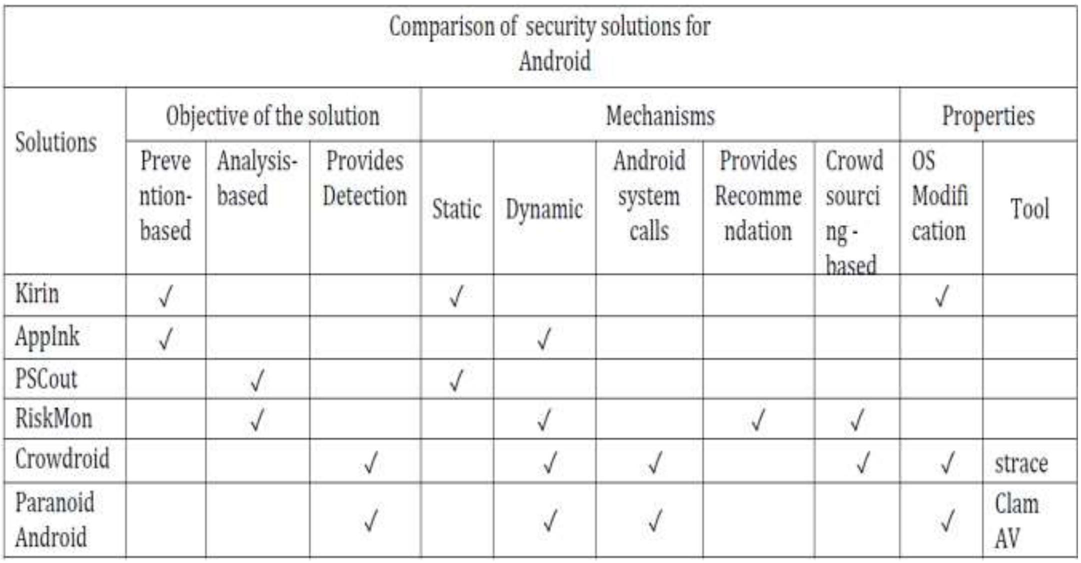

Android community with Crowdsourcing Application
Generated Output Files
Behaviour Based Malv Detection Remote Se

D. Paranoid Android

Author Paranoid Suggested security checks in Android.
The main feature of Paranoid Android is that the inspection process of the operator's device is sent to the remote control. The main reasons behind remote security checks are lack of adequate computer hardware and insufficient battery usage. It works with a remote security server, a cloud-based search framework, to host a copy of the phone in a virtual environment.As part of security, there is a two-stage process that is considered a review mechanism. In the first stage, application evaluation is carried out, followed by tool analysis. During this time, application activity is monitored and data is collected and sent to the server. System information is only shown when the device is asleep to avoid and reduce data transfer overhead. In the second step, the data collected from the device is analyzed. Paranoid Android uses ClamAV-based antivirus software to scan files.[8]

E. DroidScope

The author of DroidScope argued that he has the right to ensure that the attack can be detected even at the main level through DroidScope. Providing human analysts with a set of APIs to customize their analyticsneeds also thwarts attackers' goals of obfuscating analytics.
DroidScope is built on top of the QEMU emulator. Similarly, DroidScope is an application-oriented virtual machine introspection (VMI),dynamic analysis framework. Unlike other dynamic analysis, it does not exist in the simulator, it creates semantics at the operating system and Dalvik level from outside the simulator.
Security Solution Comparison - Android OS.[4]



Comparison of security solutions for Android

Solutions	Objective of the solution			Mechanisms					Properties	
	Prevention-based	Analysis-based	Provides Detection	Static	Dynamic	Android system calls	Provides Recommendation	Crowd sourcing -based	OS Modification	Tool
Kirin	√			√					√	
AppInk	√				√					
PSCout		√		√						
RiskMon		√			√		√	√		
Crowdroid			√		√	√		√	√	strace
Paranoid Android			√		√	√			√	Clam AV

Conclusion :-

The most used mobile operating system today is Android. Android has some technical features. However, there are threats and attacks such as malware applications on the platform. Because malware on the Android platform brings with it many dangers. The security of the Android operating system is important to protect personal information and user privacy. This article examines the security attacks and problems of the Android operatingsystem. Various solutions are a lso reviewed in this article to prevent and manage security attacks and issues in Android operating system. Some of the futurework on the Android operating system is focused on how Android security can be improved in the future.

REFERENCES :-

[1] "Smartphone users worldwide 2014-2020 | statistic," Statista," 2020. [Online]. Available: https://www.statista.com/statistics/330695/number-ofsmartphoneusers-worldwide.

[2] N. E. M. R. N. R. H. a. N. O. M. S. Ahmad, "Comparison between android and iOS operatingsystem in terms of security," in 8th International Conference on Information Technology in Asia (CITA), 2016.

[3] A. K. a. D. Upadhyay, "Modifying application's permissions and preventing information stealing on smartphones," in 5th International Conference -Confluence The Next Generation Information Technology, 2016.

[4] "Android Security," [Online]. Available: http://developer.android.com/training /articles/security-tips.html.

[5] W. L. a. R. Lee, "Multi-sensor authentication to improve smartphone security," in Conference on Information Systems Security and Privacy, 2016.

[6] A. Morris, "Multimodal person authentication on a smartphone under realistic conditions," in in Defense and Security Symposium, 2016.

[7] A. C. I. H. E. a. A. K. K. Hamandi, "Android SMS Malware: Vulnerability and Mitigation," in 27th International Conference on Advanced Information Networking and Applications, 2017.

[8] B. D. D. a. A. Zúquete, "Communications and Multimedia Security," Berlin, Heidelberg: Springer Berlin Heidelberg, vol. 8735, 2015.

[9] D. K. M. P. a. S. C. H. Lee, "Protecting data on android platform against privilege escalation attack," International Journal of Computer Mathematics, pp. 1-14, 2015.

[10] W. H. a. Y. L. Z. Fang, "Permission based Android security: Issues and countermeasures," Computers &Security, vol. 43, p. 205–218, 2016.

[11] "Android data leakage," [Online]. Available: http://www.appstechnews.com/news/2016/oct/25/research-revealsios-and-android-app-data-leakage-and-what-it-means-enterprises/.

[12] A. F. a. S. C. C. Marforio, Application Collusion Attack on the Permission-Based Security Model and Its Implications for Modern Smartphone Systems, 2010.

[13] E. Kovacs, "flaw exposes android devices to dos attacks," [Online]. Available: http://www.securityweek.com/wi-fi-directflaw-exposes-android-devices-dos-attacks.

[14] S. Z. P. L. a. D. W. H. Huang, "A framework for evaluating mobile app repackaging detection algorithms," in Proc. of the 6th International Conference on Trust and Trustworthy Computing.

[15] G.-J. A. Z. Z. a. H. H. Y. Jing, "Riskmon: Continuous and automated risk assessment of mobile applications," 4th ACM Conference on Data and Application Security and Privacy (CODASPY'14), p. 99–110, 2016.

[16] M. O. a. P. M. W. Enck, "On lightweight mobile phone application certification," 16th ACM Conference on Computer and Communications Security , p. 235–245, 2015.

[17] I. B. a. U. Zurutuza, "Crowdroid: Behavior-Based Malware Detection System for Android".

[18] K. A. G. P. Philip Homburg, "Paranoid Android: Versatile Protection for Smartphones".

[19] L. K. Y. a. H. Yin, "Droidscope:Seamlessly reconstructing the os and dalvik semantic views for dynamic android malware analysis," in 21st USENIX Conference on Security Symposium, 2015