Survey Paper on Unmasking & Forfending Malware Techniques in Android

Komal Patel[1], Gayatri Pandi[2]
[1, 2] Department of Computer Engineering
[1, 2] LJIET

Abstract- *The ruling smartphone platform nowadays is an Android. The open source feature of this operating system lead to malware creators to introduced new malware each day and are avoiding the possibility of unmasking and forfending the malicious code available in the software or application and manipulate users' private information without their knowledge. Malwares are made to introduce many different cybercrimes such as misuse of services, sucks the information, and root or kernel access of the device. There are several methods are introduced by many different research to avoid such situation by unmasking such malicious activity and forfend future risks of malware and provide a safe environment for the Android smart phone users. The paper discusses the type of malware and methods to unmask and forfend their activity.*

Keywords- Android Architecture, Malware, Security, Techniques.

I. INTRODUCTION

Android is most popular mobile operating system in 2015-16. According IDC (International Data Corporation), Second half of 2015 average 81.95% and in first half of 2016 on average 85.5% is the market share for the Android operating system.

The different versions of Android are shown in below figure.

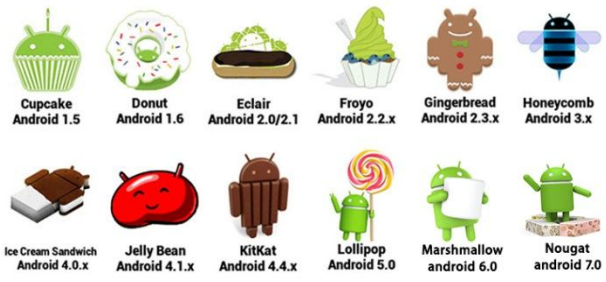

Fig 1 : Different Versions Of Android Operating System[6]

The main reason behind the popularity of Android operating system is its open source and many other unique features such as Beautiful UI, Connectivity, Storage, Media support, Messaging, Web browser, Multi-touch, Multi-tasking, Multi-tasking, Resizable widgets, Multi-Language, GCM, Wi-Fi Direct and Android Beam.

Android application components can be divided into major four parts:

1. Activity: It is the user interface component of an app. Any number of activities can be startedinmanifest file based on the developer requirements. An activity can also return the result to its caller. Activities are launched using the Intent. Only one activity is possible to activated at a time, other are suspended at that time.

2. Service: Service component performs background tasks without any UI. For example, playing an audio or download data from the network are background processing. Services are launched using Intents. There are number of services running in the background which cannot be tracked by user himself.

3. Broadcast Receiver: This component listens to the Android system generated events. They store and share data via relational database. For example, SMS_SENT etc. is system events. Any application registered their affiliation with this can access it.

4. Content Provider: Content provider also known as the data-store, provides a consistent interface for data access between within and between different apps. They responds to system-wide broadcasts. Broadcast classes are: I) Normal Broadcasts and II) Ordered Broadcasts.[2]

The permissions provided by Android can be divided in mainly four types:

1. Normal permissions
2. Dangerous permissions
3. Signature permissions
4. Signature Or System permissions[7]

The of paper is organized as below: Section II discuss about 3 approaches to unmask and for fend it. Section III describes literature survey of different researches. Section IV Conclude the survey.

II. MALWARE

The popularity also attracts the malware writers. The come up with new and different techniques each day which leads to many cyber-crimes, fraud, information stealing, privacy leakage of user.

Malware can be formally classified as follows:

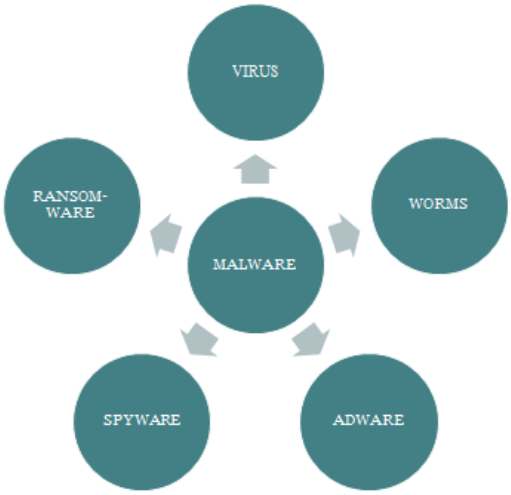

Fig 2: Classification of Malware

Malware is kind of software that harm & infect the computer system or mobile system. Each day new kind of malware are introduced thus to unmasking and for fending techniques should be adoptive to the stubborn nature of malwares.

Malware can be mainly classified in five types:

Virus is type of virus that can able to spread it; it is a piece of code and affects other software. Adware is type of malware based on advertising software and websites. It generates revenue for its writer, also track users internet logs. Spyware is most difficult malware to detect. It spies user, track their activities in the system, gather important and confidential information and manipulate according to requirements. Worms are replicatin git. They are able to access root and destroy information, files or even operating system itself. Ransomware is the most advanced malware till now. It locks your files, data or PC and extorts money from you in order to provide access to collect funds for their legitimate activities in the web

III. APPROACHES TO UNMASK & FORFEND EFFECT OF MALWARE

The malware analysis and unmasking techniques can be classified into three categories:

1) Static Analysis
2) Dynamic Analysis
3) Hybrid Approach[2]

In static analysis, Signature-based, Permission-based, and Component-based analysis is performed. In first analysis method it pull out the syntactic or semantic patterns or features& define unique signature to compare other malware, in second it checks defined permissions by the application and distinguish dangerous permission, and in third disassembles targeted software or application to pull out and dissect the definition and byte code interaction of android application components to define the vulnerabilities.

In dynamic analysis, applications are deployed and executed on an emulator or a controlled device to define different behaviors of malware. It needs to act like users' behavior and also it needs human-like inputs. The issue with this method is resource consumption due to continuous detection for the malicious code.

In hybrid approach, the favorable conditions for both the analysis approach are combined.

IV.COMPARITIVE STUDY FOR SOME SURVEYED PAPERS

Sr No	**Paper Title**	**Method Used**	**Pros**	**Cons**
1	A detection method for malicious codes in android apps[1]	Static and dynamic analysis.	More accurate result, real-time monitoring of behavior	Large consumption of resources and time.
2	Dissecting SMS Malwares in Android[2]	SMS service as RogueSms' medium of operation, delete notification when it received on user device.	Behavior based detection is allowed	Intent delivery is compulsory, same parameter for each can not detect malicious activity.

3	Detection and Identification of Android Malware Based on Information Flow Monitoring[3]	Create SFG to detect malicious activity in information flow	100% TPR and TNR	Detect only predefined malware families
4	Detecting and tracing leaked private phone number data in Android smartphones[4]	Virtual phone number for each suspected application.	Can avoid voice phishing or SMS phishing by using proxy server	scalability problem in terms of Cost
5	Prevention Mechanism for Prohibiting SMS Malware Attack on Android Smartphone[5]	Mathematical model for detection & prevention	Detect and prevent application to send data to C&C.	Behavior based malware can not be detected

VI. CONCLUSION

The existing smartphone security models facilitate mechanisms and processes controlling the installation and execution of third party applications. Even so, the sufficiency of the adopted security mechanisms seems to be controversial. Their ability to protect the users' data is big concerned. The paper focuses on different method to unmask the malware and also provide some comparative study of previous research work on same issue.

REFERENCES

[1] Liu, Jinxin, Hao Wu, and Huabin Wang. "A detection method for malicious codes in Android apps." In Wireless Communications, Networking and Mobile Computing (WiCOM 2014), 10th International Conference on, pp. 514-519. IET, 2014

[2] Babu, Anoop Joseph, Rahul Raveendranath, VenkiteswaranRajamani, and SoumyaKantiDatta. "Dissecting SMS malwares in android." In Contemporary Computing and Informatics (IC3I), 2014 International Conference on, pp. 1065-1069. IEEE, 2014

[3] RadoniainaAndriatsimandefitra, Val´erie Viet Triem Tong, "Detection and Identification of Android Malware Based on Information Flow Monitoring" In 2nd International Conference on Cyber Security and Cloud Computing, Pg: 200-203, IEEE, 2015, DOI:10.1109/CSCloud.2015.27

[4] Wooguil Pak, Youngrok Cha, Sunki Yeo, "Detecting and tracing leaked private phone number data in Android smartphones",31st International Conference On Information Networking(ICOIN), Pg:503-508, IEEE, 2015, DOI:10.1109/ICOIN.2015.7057956

[5] Kotkar, Chetan, and Pravin Game. "Prevention mechanism for prohibiting SMS malware attack on android smartphone." In 2015 Annual IEEE India Conference (INDICON), pp. 1-5. IEEE, 2015

[6] https://www.google.co.in/imgres?imgurl=https%3A%2F%2F4.bp.blogspot.cm%2FgJgio2rWQGA%2FV8WpJZ9HXcI%2FAAAAAAAACSg%2F24jB0Qbej7sg_volhVsb4G092_UEfTwCLcB%2Fs1600%2Fandroid_nougat_new_android_addition.jpg&imgrefurl=http%3A%2F%2Fshaourhaider.blogspot.com%2F2016%2F08%2Fhavenougatandroidn.html&docid=s4UZwWGRXjCU5M&tbnid=8xxv3dJemrUdM%3A&vet=1&w=729&h=400&bih=662&biw=1366&ved=0ahUKEwiwoYLt5uHQAhWCGpQKHf0hAIUQMwgiKAYwBg&iact=mrc&uact=8 accessed on dec 2, 1:00pm

[7] https://developer.android.com/guide/topics/manifest/permission-element.html accessed on nov 25, 8:30 am