International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 4: April 2016, pp 48-51. www.aetsjournal.com ISSN (Online) : 2394-6237

Survey on Mobile Malware Detection Techniques in Android Operating System

S. Birundha, Dr. V. Vanitha,

Abstract— The extensive use of mobile devices has led to a new era of change in everyday life. Mobile devices are more powerful and are very portable when compared to Personal Computers (PC's). The rise in the smart phone usage resulted in the raise in mobile malware targeting the Android platform. Due to abundant instances of security attacks and privacy leakage on Android platform, security in Android has been a hot spot in the academic research as well as in public concerns. . In addition, the rise of mobile malware that spread via SMS/MMS messaging and Bluetooth makes possible malware outbreak which closely tracks the progress of human mobility patterns, hence new and novel detection methods are required. This paper presents a comprehensive review that broadly discusses the mobile malware and briefly summarizes the previously published studies. The survey also discuss about various methods for detecting mobile malware in Android platform.

Keywords -Mobile malware; Smartphone; Security; Malware detection

I. INTRODUCTION

Mobile technology has extended dramatically around the world. These days' smart mobile devices are used for various purposes like personal mobile communication, data storage, multimedia, financial transactions and also for the entertainment. Today, Android is a popular mobile operating system, the reasons for being favored by users are listed as, (1) Open source software (2) being supported by Google (3) applications being developed in the most popular programming language Java (4) being open for the customization. Thus, Smartphone usages have brought new era of information exchange to everyday life. The number of mobile malware is increasing speedily with various malicious activities such as, stealing users' personal data, sending premium messages and making calls without the users' acknowledgement. These malicious activities are hidden from the user and they run in the background. Numerous studies have developed methods to detect such attacks.

Juniper Networks in their third annual Mobile threats report [1] has stated that malware intended to attack specifically the Android devices and it has increased at an alarming rate since 2010. Cisco's 2014 Annual Security Report has affirmed that 98% of mobile malware software's objective is to target the Android platform [2]. According to F-Secure, a cyber security associated company, the number of new mobile malware families and variants continued to increase by 49% and 91.3% of these malware being targeted at Android devices in the first quarter of 2013[3]. In order to prevent users from these malicious activities, malware detection in Android operating system is very much essential and necessary. The solution providers of Android security stated that there is an alarming rise of malware and thus the malware authors use different techniques to override the existing security mechanisms provided by the Android platform. This paper discusses about the survey of various malware analysis and malware detection techniques and the need for malware detection. The exponential increase in the malware applications has enforced the malware developers to design the robust and efficient detection techniques. The existing Signature based methods can be easily evaded by the malware.

This paper describes about the need for malware detection in Android operating system and the survey of malware detection techniques. Section II discusses about the need for mobile malware detection, Section III explains the Android malware threat. Section IV deals with the different Android malware detection techniques. Section V concludes the paper.

II. NEED FOR ANDROID MALWARE DETECTION

Android operating system has the maximum market share in the year 2014, which makes it the most extensively used operating system in the world. This makes the Android users the biggest target group for malware developers. Permission based mechanism plays an important role in Android security, which restricts the accesses of third-party Android applications to significant resources. A piece of Android malware can rise privileges by sending short service messages, by making calls to premium numbers, sharing local information through Global Positioning System(GPS), and finally collects excessive amount of information without the users' knowledge. The need for Android malware detection is increased as security mechanism in Android does not set limit on the system resource usage. This is a critical susceptibility point for malicious applications.

III. ANDROID MALWARE THREAT

This section describes about the Android device security issues and the reported Android device threats. Following are the listing of various malicious activities that are employed across different Android versions. Personal information theft occurs when the users grant permissions to malicious

S. Birundha Dept. of computer science and engineering, Kumaraguru College of Technology, Coimbatore, India. (Email: mailtobrindha@gmail.com)
Dr. V. Vanitha, Dept. of computer science and engineering, Kumaraguru College of Technology, Coimbatore, . (Email: vanitha.v.cse@kct.ac.in)

applications. Malicious applications can also steal users sensitive data without the user knowledge records the voice calls and earn money by subscribing to the premium rate numbers and start sending messages. Denial of Service (DoS) attack may also happen when the application over uses the CPU, battery, memory and the available bandwidth resources. In the following paragraph, the various Android malware and its characteristics are listed.

- Trojan – Android malware which performs malicious and dangerous activities by phishing the user to steal the sensitive information such as username and password. The harmful activities performed by this malware are unseen to the users' knowledge. FakeNetflix, Fakeplayer[5] are some prominent Android Trojans which gives various financial loss to the user.
- Backdoor – Backdoor tries to gain the root privilege of the users and then bypass the normal security procedures. This malware acquire the super user privilege i.e., full control of the device and performs malicious activities. Kmin, Basebridge [6] are some of the examples of backdoors.
- Worm – Worm spread through the network or media by generating the copies of itself. For instance, Bluetooth worms.
- Botnet – This type of malware compromise the mobile device for the creation of Bot, and the device is controlled remotely. The remote server is called as the Botmaster and it sends series of commands to perform harmful activities. Geinimi [6], Anserverbot [6] are few Android botnets.
- Adware – This type of malware mistreats the network and gets location services. By knowing the location services, adware creates the shortcut on the home screen and sends superfluous notifications to thwart the effective device usage. Plankton is a best known aggressive adware.
- Ransomware – This malware locks the user device, only if some amount is paid as an online payment, the device will be unattainable.

IV. ANDROID MALWARE DETECTION TECHNIQUES

Android applications comprises of different variety of features. In order to develop an effective detection system, subset of features has to be chosen from the available features. Ali Feizollah et al.[4] presented a paper on the review of mobile malware features. Android malware detection includes analysis on static features, dynamic features and hybrid features. Static features includes features available in the .apk(Application Package) file. The file includes Androidmanifest.xml file comprises of permission feature, java code feature, hardware components, intent filters, strings and network address. Android applications are packaged in to an APK file which is a zip archive comprising of a number of files and folders which is illustrated in Fig 1.

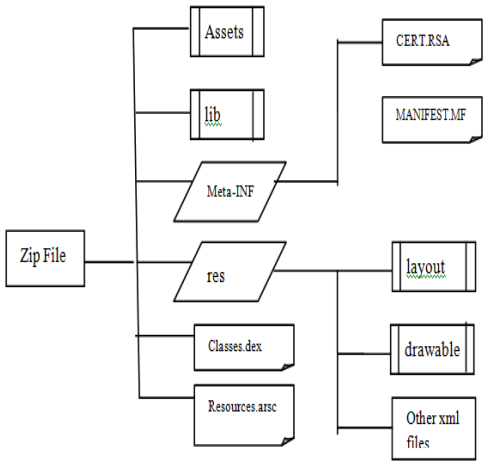

Fig 1 – Android Package Structure

Dynamic features include network traffic, system call feature, System components and user interactions. Hybrid feature includes the combination of static and dynamic features.

A. Static Analysis method

Static analysis based malware detection approach does not have an effect on the device as this approach works by decompilation and disassembly. Hence this approach is quick but has to deal with the false positives. Signature based malware detection is one of the method used to detect the malware based on the unique signature that matches the already existing and known malware. Dong-Jie Wu et.al. [7] proposed a system called DroidMat, a static analysis based malware detection system. This system extracts the important information such as, permissions, application behavior using the API calls, intent messages, etc. Arp et.al.[8] Proposed a tool called, Drebin, a light-weight approach used to detect Android malware. This method combines the static analysis approaches and machine learning based methods. For the detection of malware, Drebin used Support Vector Machine (SVM), machine learning algorithm and the results showed that the method detects 94% of malware. Wu et al. [9] proposed Droidmat, in which features are extracted including intent filters and machine learning algorithms are applied for the detection of malware.

Permission based analysis of malware detection plays a significant role in malware detection as Android security framework is built on the permissions the applications use. Zheran Fang et.al. [10] Proposed permission based Android security and illustrated the relationships among various issues in the Android security. The relationship among different permissions is shown in Fig 2.

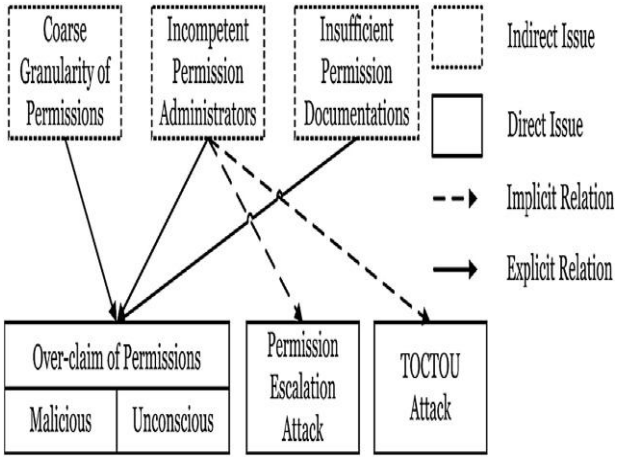

Fig 2 – Relationship among issues in Android permission mechanism

Kirin [11] project developed a tool to identify the permissions which helps to identify the malware attributes that makes harmful activities. This method provides a light weight mobile phone certification. The sample AndroidManifest.xml file used for the permission based malware detection is shown in Fig 3.

Fig 3 – Sample AndroidManifest.xml file

Kabakus Abdullah Talha et.al.[12] Presented APK Auditor, a permission based malware detection approach. APK Auditor comprises of three components, An Android client, signature database, and central server for communication purposes.

B. Dynamic Analysis method

Static analysis and detection methods are simple, quick and efficient but fail to identify the new and self-updating capability malware. On the other hand, dynamic analysis and detection run the applications in a protected environment and thus learns the interactions of different malicious activities made by the malware. But Smartphone's resource constraint limits dynamic analysis methods. Shabtai et.al. [13] Proposed a tool named Andromaly, which is an Android malware detection tool and is light-weight application. This system performs the real-time supervising for the gathering of various system metrics such as the usage of battery, CPU consumption by the application, network utilization and the active processes. Andrubis [14], a web-based malware analysis platform and is built upon various tools such as, DroidBox, apktool and Androguard. Crowdroid [15], behavior based malware analysis and detection approach, which accumulate the system call using the Strace tool and detects the presence of malware. Reina et al. [16] proposed a tool named, CopperDroid, performs dynamic analysis of Android apps based on system call-centric using Virtual Machine environment. Droidbox [17] tool for the dynamic analysis of malware detection, developed on the basis of Taintdroid [18] and the goal of this tool is to monitor and to do taint analysis.

V. CONCLUSION

Malware analysis and detection has become more significant due to the exponential increase in the number of unknown and new malware samples. In recent years, Android security has become more severe, due to vulnerabilities in the Android system design and a big success of Android device in the market place, which motivated to provide a systematic overview of the recent research in Android security. From the previous studies and research work it can be concluded that Mobile malware has specific network flow characteristics in which repeated communication occurs between Android OS and infected machine. To detect mobile malware, application network behavior analysis, decision fusion approach, permission based Android security, kernel based mechanism have been implemented already. As new malwares are evolving every day, it is important to enhance the detection techniques at the installation time.

REFERENCES

[1] Juniper Networks Mobile Threat Center. Third Annual Mobile Threat Report: March 2012 to March 2013, URL ⟨http://www.juniper.net/us/en/local/pdf/ additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf⟩, 2013.

[2] Cisco 2014 Annual Security Report, URL ⟨http://www.cisco.com/web/offer/ gist_ty2_asset/Cisco_2014_ASR.pdf⟩, 2014.

[3] F-Secure. Mobile threat report January-March 2013 http://www.fsecure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2013.pdf.

[4] Ali Feizollah, Nor Badrul Amitar, Rosli Salleh, Ainuddin Wahid Abdul Wahab, : A review on feature selection in mobile malware detection", Digital Investigation, 13 (2015) 22-37.

[5] G. Andre, P. Ramos, BOXER SMS Trojan, Tech. rep., ESET Latin American Lab (2013).

[6] Z. Yajin, J. Xuxian, Dissecting Android Malware: Characterization and Evolution, in: Proceedings of the 33rd IEEE Symposium on Security and Privacy, Oakland 2012, IEEE, 2012.

[7] Dong-Jie Wu, Chiang-Hao Mao,Te-En Wei,Hahn-MingLee,Kuo-Ping Wu, "DriodMat:Android Malware Detection through Manifest and API calls Tracing", Information Security(Asia JCIS), 2012 Seventh Asia Joint Conference, pp 62-69

[8] Arp D, Spreitzenbarth M, Malte H, Gascon H, Rieck K. Drebin: effective and explainable detection of Android malware in your pocket. In: Symposiumon network and distributed systemsecurity (NDSS); 2014.

[9] Wu D-J, Mao C-H, Wei T-E, Lee H-M, Wu K-P, "Droidmat: android malware detection through manifest and api calls tracing. In: Seventh Asia Joint Conference on Information Security (Asia JCIS). IEEE-2012.

[10] Zheran Fang, Weili Han, Yingjiu Li, "Permission based Android security: Issues and countermeasures", computers & security 43 (2014) 205- 218

[11] W.Enck,M.Ongtang,P.McDaniel, "On lightweight mobile phone application certification", in:Proceedings of the 16th ACM Conference on Computer and Communications Security, ACM, Chicago, IL, USA,2009,pp.235–245.

[12] Kabakus Abdullah Talha, Dogru Ibrahim Alper , Cetin Aydin, "APK Auditor: Permission-based Android malware detection system, Digital Investigation 13 (2015) 1-14.

[13] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, Y. Weiss, "andromaly": a behavioral malware detection framework for android devices., J. Intell. Inf. Syst. 38 (1) (2012) 161–190.

[14] Andrubis (2012). URL http://anubis.iseclab.org/

[15] I. Burguera, U. Zurutuza, S. Nadjm-Tehrani, Crowdroid: Behaviorbased Malware Detection System for Android, in: Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, ACM, 2011, pp. 15–26.

[16] A. Reina, A. Fattori, L. Cavallaro, "A System call-centric analysis and stimulation technique to automatically reconstruct Android malware behaviors ", EUROSEC, Prague, Czech Republic.

[17] A. Desnos, P. Lantz, Droidbox: An android application sandbox for dynamic analysis (2011). URL https://code.google.com/p/droidbox/

[18] E. William, G. Peter, C. Byunggon, C. Landon, "TaintDroid : An Information Flow Tracking System for Real-time Privacy monitoring on Smart phones", in: USENIX Symposium on Operating Systems Design and Implementation, USENIX, 2011.