A survey on Mobile Threats and Detection Techniques

Gulshan Kumar[#1], Manisha Batra*[2], Sheenam Bhola[3]
[#]*Department of Computer Applications, SBSSTC Ferozepur*
Punjab, India (152004),
[1]gulshanahuja@gmail.com
[3]sheenambhola@gmail.com
*Dept of Computer Applications, SBSSTC, Ferozepur-India (152004)
[2]manisha.batra7@gmail.com

Abstract - **In the past few years, the market adoption and utility of mobile devices has expanded intensely. Mobile devices store personal details like contacts and text messages. Due to this widespread growth, smart-phones are attracted towards cyber-criminals. Mobile phone security has become an important characteristic of security issues in wireless multimedia communications.In this research work, we have done a methodical review of the terms related to malware detection algorithms and have also a concise, interactive explanation of some known mobile malware in tabular form. After careful study of all the possible procedures and algorithms for detection of mobile-based malware, we give some recommendations for designing future malware detection algorithm by considering computational complexity and detection ration of mobile malware.In this paper, we will discuss mobile device attacks and types of detection techniques for mobile malware. At the end of this chapter we will give a conclusion by analyzing various techniques proposed by different researchers followed by some future recommendations.**

Keywords **- Smart-phones, Malware, Attacks, Static Analysis, Dynamic Analysis.**

I INTRODUCTION

At the present time, smartphones and other mobile devices are playing an imperative role in how people are entertained, network, communicate, shop, bank, and work. Nowadays, there is a very less difference between Smart-phones, Personal Computers and other devices like laptops and tabs as they all are now linked technologies. Due to the various services provided by Smart-phones like social networking and gaming, these are gaining some confidential information from mobile devices. The modern Smartphone platforms include Symbian, Android, iOS, PalmOS and embedded Linux, etc. Android is the most popular platform for smart-phone based malware authors. By installing malicious content, smart-phones can also be infected with worms, trojan horses or other virus families, which can compromise the user's security and privacy or even gain complete control over the device. So, it requires special care to secure these networked devices from malware with the help of anti-developed techniques and algorithms for detection. Researchers from Kaspersky Lab first found the malware called Cabire, for mobile phone in 2004. After that number of malware increased largely along with the popularity of the smartphones [11-13]. This paper discusses about mobile malware and analysis of different mobile malware detection techniques.

II MOBILE MALWARES

Unfortunately, you may know about the viruses that can attack your computer, but what about the viruses aimed at your mobile devices? You may be surprised to learn that malicious software aimed at mobile devices, otherwise known as mobile malware, is on the rise, yet two thirds of smartphone owners don't even realize their device can be infected [1]. Malware aimed at Android smartphones alone has grown 76% over the last few months, threatening Android security, and other platforms are also coming under attack. Many of the threats, such as clicking on a dangerous link in an email or in search results, are the same as you would encounter on your computer, but there are other threats that are unique to mobile devices [6].

III MOBILE DEVICE THREATS

Like viruses and spyware that can infect your PC, there are a variety of security threats that can affect mobile devices. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including cyber criminals, hackers, foreign nations engaged in espionage, and terrorists. Mobile threats are divided into several categories: application based threats, web based threats, network based threats and physical threats as depicted in Figure 1 [1,15].

© 2014 JCT. All Rights Reserved

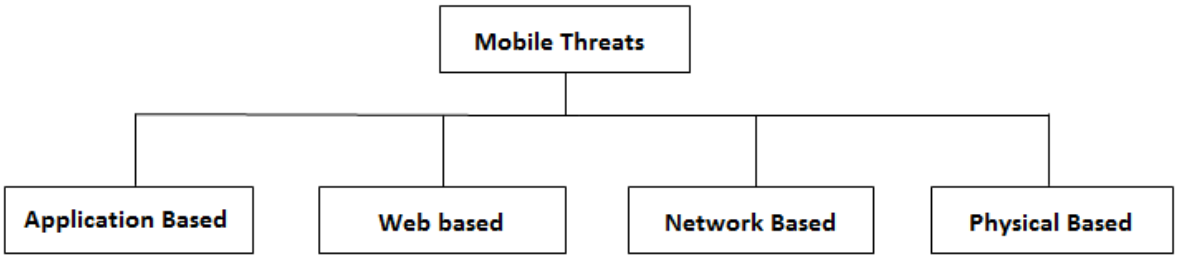

Fig 1: Various Mobile Threats

APPLICATION BASED THREATS:

Application-based threats generally fit into one or more of the following categories:

- **Malware:** Malware is a type of malicious software that performs malicious actions while installed on your phone., that attempt to make changes on your phone bill, send malicious messages to your contact list or given to the attacker control over your mobile smartphone device without your knowledge. Some of the malware attacks are listed as:
  a) **Bluetooth attacks:** With Bluetooth attacks, an attacker could insert contacts or SMS messages, steals victim's data from their devices and can track user's mobile location. The blue-bugging is a kind of Bluetooth attack through which attacker could hear conversations by activating software including malicious activities.
  b) **SMS attacks:** With SMS attacks, an attacker can promote and spread phishing contacts. SMS messages can also be used by attackers to adventure susceptibilities.
  c) **GPS/Location attacks:** With the help of global positioning system (GPS) hardware, user's current location and movement can be accessed. After this, information can be sold to other companies involved in advertising [1,15].
- **Phone jail-breaking:** With jail-breaking, an attacker can remove security implications of operating system like it allows an operating system to install additional and unsigned applications. Users are attracted to install them as they could get additional functionality [3].
- **Spyware:** Software designed to accumulate private data without the awareness or support of the user. The common data targeted by the spyware includes phone call histories, text messages, user location, contact list, private photo and all the information that could be useful for the attackers to commit a financial scam or an identity theft.
- **Privacy Threats:** This can be caused for applications that are not properly malicious, but use sensitive information as location, contact list, personal information that is essential to implement their function [3,4].

WEB BASED THREATS:

Mobile devices are constantly connected to the internet and used to access web based services. Web based threats that affect PCs can also prevent issues for mobile devices [4,5].

- **Phishing Scams:** Phishing scams use e-mail, text messages, Facebook and twitter to send you links to websites designed to trick you providing personal information like passwords or account numbers.
- **Drive-by Downloads:** This can automatically download an application when you visit a web page. In some cases, you must take an action to open the downloaded application, while in other cases, the application can start automatically.
- **Browser exploits:** It is designed to take an advantage of weaknesses in your mobile software that can be launched directly by the browser such as the Flash player, PDF reader, or image viewer etc [2,3].

NETWORKING THREATS:

Mobile devices support cellular networks as well as local wireless networks (WiFi, Bluetooth, GSM etc.). These types of networks can host different classes of threats:

- **Network exploits:** Exploits that take advantage of flaws in the mobile operating system, software that operates on local or cellular networks and once connected, they can install malware on your phone without your knowledge.
- **Wi-Fi Sniffing:** These are attacks that consist on data interception when are travelling through the air, between the device and the Wi-fi access

© 2014 JCT. All Rights Reserved

point [8, 9]. In locations, the web pages don't use encryption when send data across the network and these can become easy to read by someone who is grabbing them as it travels.

PHYSICAL THREATS:

Mobile devices are small, valued and we can carry them everywhere with us. We use it for both personal and professional purposes. Our phones could contain sensitive data, so their physical security is also important.

- Lost or stolen devices: The mobile device is valuable not only because the hardware itself can be re-sold on the black market, but more importantly because of the sensitive personal and organization information it may contain.
- Internet Access: Mobile devices can access the Internet using WiFi networks or 3G/4G services provided by mobile network operators. Although such high speed Internet connections ensure comfortable browsing, they also expose the mobile devices to the same threats as PCs. Since mobile devices are usually constantly switched on, they can maintain a continuous connection to the Internet [8,9]. However, prolonged connection to the Internet also increases the chances of a successful malicious attack.

IV MALWARE DETECTOR:

The malware detector is those who always help to protect the system by detecting malicious behavior. The malware detector performs its protection through the manifested malware detection techniques. Malware detectors take two inputs. One input is its knowledge of the malicious behavior; this knowledge comes from the learning phase [10]. The other input is the program under inspection. Once the malware detector has the knowledge of malicious behavior and the program under inspection, it can employ its detection techniques to decide if the program is malicious or not.

MALWARE DETECTION TECHNIQUES

In this section, we analyze various mobile malware detection techniques from various research papers.

STATIC ANALYSIS

Static analysis is a quick, economical approach to finding malicious features or bad code segments in an application without executing them. These techniques are used in a preliminary analysis, when doubtful applications are first evaluated to detect any security threats [10].

System Call: The mobile application is first dissembled using tools like IDA pro. The tool is used to extract the System calls made by the application and then passed to Centroid Machine to perform anomaly detection and classify application based on the malicious activities (refer Figure 2 and 3).

- Source code analysis: This malware detection technique was proposed for Android. This approach uses ded, a Dalvik Decompiler to generate Java source code from the application's installation image and then use Fortify SCA, a static code analysis suite, to evaluate the recovered source code [10,11].

DYNAMIC ANALYSIS

The dynamic monitoring the activities of mobile application in an isolated environment is known as Dynamic or Behavioral Analysis. Previously, Researchers use dynamic analysis in system call tracing. TaintDroid provides system-wide dynamic taint tracking for Android. The mobile application passes to the Dalvik Virtual machine to perform four granularities of foul transmission: method, message, file-level and variable. Taint tracking marks any uncertain data that starts from sensitive sources, such as microphone, camera, location, and other phone identifiers. This technique modifies the native library loader to ensure that all the native libraries are called from the virtual machine, thus preventing untrusted applications from executing native methods directly. Finally, dynamic analysis screens impacted data for any potentially sensitive data leaks before it leaves the system at the network interface. TaintDroid might suffer from false negative and false positive results; in addition, it focuses solely on dataflow and doesn't consider other vulnerabilities. The Android Application Sandbox (AASandbox) system is another technique which offers two-step analysis for an Android application. A mobile application passes to AASandbox, where it performs static and dynamic analysis in offline mode [10,11]. Static analysis disables the application image binary and uses the disassembled code to search for suspicious patterns. Dynamic analysis executes the binary in an Android emulator and logs the system calls.

APPLICATION PERMISSION ANALYSIS:

Applications need some permission to access certain data. At the time of installation, Android platform asked the user to grant or deny permissions based on the activities the application can perform. The below Figure 4 shows Kirin security service for the Android platform [11]. Kirin performs a permission check on the application during installation. When a user installs an application, Kirin extracts its security configuration and checks them against the security

© 2014 JCT. All Rights Reserved

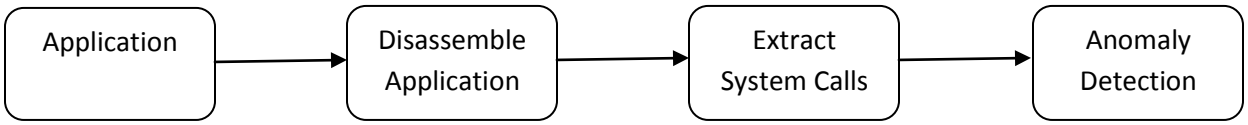

Fig 2: System Call

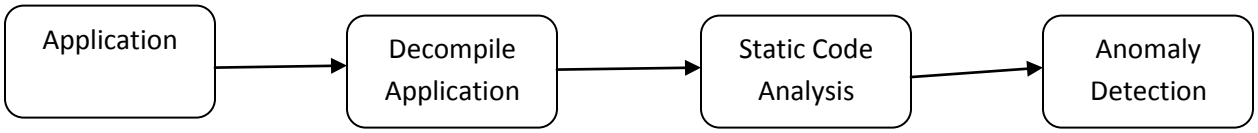

Fig 3: Source Code Analysis

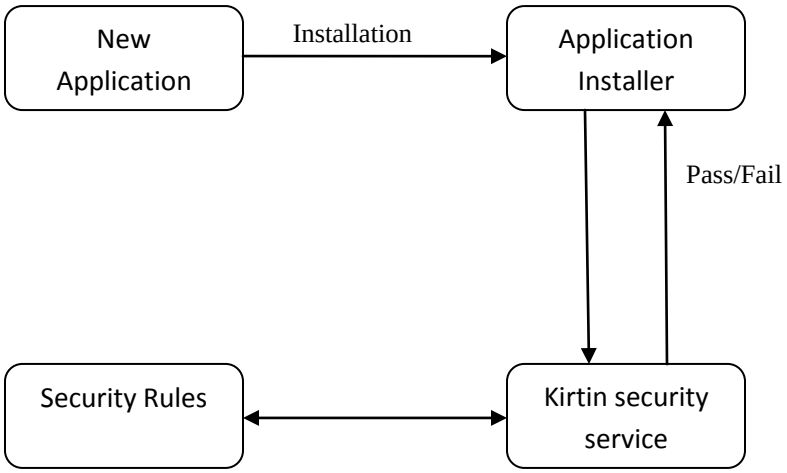

Fig 4: Application permission Analysis

policy rule that it already has. If an application fails to pass all the security policy rules, Kirin can either delete it or alert the user.

BATTERY LIFE MONITORING:

As malicious application tend to use most of the battery capacity. An interesting methodology VirusMeter was proposed by Liu et al to detect energy consumption and detect malware. VirusMeter detects anomalous behavior by abnormal power consumption. The idea behind this approach is any malicious activity would consume more battery [14]. VirusMeter monitors the activities in the phone and uses APIs provided by the mobile platform to collect the remaining battery capacity. Based on the collected data it computes how much the application can consume battery and compares it with the power model. If there is a difference and if it exceeds the threshold then it raises alarm.

V CONCLUSIONS

Modern, smartphones provides lots of services such as messaging, browsing internet, emailing, playing games in addition to traditional voice services. Due to their flexible addition and communication capabilities, mobile handsets are fastened victim to malware. This paper presented and analyzed some of researchers' effort on that aspect. In this paper, we presented a survey on various techniques for detection of mobile malware. There are various mobile malware detection techniques based on features extracted from them. These techniques handle several kinds of structurally different malware, which are produced by employing complication techniques. Some limitations of dynamic analysis like single execution path, significant performance overhead, etc. make static analysis more superior than dynamic. Mainly the focus of this paper is on employing such an analysis technique for malware which overcome the limitations related to the existing counterpart techniques.

© 2014 JCT. All Rights Reserved

REFERENCES

1. Dua. L and Divya Bansal "Review on Mobile Threats and Detection Techniques", International Journal of Distributed and Parallel Systems (IJDPS) Vol.5, No.4, July 2014, online available: http://airccse.org/journal/ijdps/papers/5414ijdps03.pdf
2. Networks Inc. Malicious mobile threats report 2010/2011. Technical report, Juniper Networks, Inc., 2011.
3. Aubrey-Derrick Schmidt, Ahmet Camtepe, and Sahin Albayrak. Static smartphone malware detection. In proceedings of the 5th Security Research Conference (Future Security 2010), ISBN: 978-3-8396-0159-4, page 146, 2010.
4. D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: The viruses are coming!" IEEE Pervasive Computing, vol. 3, no. 4, pp. 11-15, 2004.
5. H.Kim, J.Smith, K.G. Shin,:Detecting energy-greedy anomalies and mobile malware variants: In MobiSys 08: Proceeding of the 6th international conference on Mobile systems, applications, and services, pp. 239-252.ACM,NewYork (2008).
6. M.L.Polla,F. Martinelli, D. Sgandurra: A Survey on Security for Mobile Devices: Communications Surveys and Tutorials, pp.446-471.IEEE (2013)
7. Dr. Mirzoev.T, Brannon. M, Shamimara Lasker, Mark Miller "Mobile Application Threats and Security", World of Computer Science and Information Technology, ISSN: 2221-0741
8. http://mysecurityawareness.com/article.php?article=282&title=keep-your-mobile-device-secure-from-malware#.VFT5MfmUfvI
9. Sophos,"SecurityThreatReport,"2010.[Online]: http://www.sophos.com/sophos/docs/eng/ papers/sophos-security-threat-report-jan-2010-wpna.pdf
10. Aswathy Dinesh," AN ANALYSIS OF MOBILE MALWARE AND DETECTION TECHNIQUES",online available: http://tuftsdev.github.io/DefenseOfTheDarkArts/students_works/final_project/adinesh.pdf
11. Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra," A Survey on Security for Mobile Devices", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO.1, FIRST QUARTER 2013.
12. Erica Ogg, "HP: Number of mobile application doesn't matter," CNET News, June 29, 2011
13. Ramu, S. "Mobile Malware Evolution, Detection and Defence", April 2012.
14. Liu, L. G., Zhang, Y, X., Chen. S. "VirusMeter: Preventing your cellphone from spies" In Proceedings of RAID, volume 5758 of Lecture Notes in Computer Science, 2009.
15. Sujithra. M, Padmavathi. G "Mobile Device Security", International Journal Of Computer Applications (0975-8887, *Volume 56– No.14, October 2012*.

© 2014 JCT. All Rights Reserved