Is your Mobile App Safe? Mobile App Attacks and Defense

1. Kireet Muppavaram, External Research scholar, Lecturer, JNTUCEH, kireet04@gmail.com
2. Kaavya Rekanar, Researcher, Blekinge Institute of Technology, Sweden, kare15@student.bth.se

***Abstract*—Usage of mobile phones has increased over the years, all over the world. With the extensive usage of smartphones, it has been confirmed by that most of the smartphone users work in an Android platform as it is an open platform which can be used by anyone to develop applications or introduce malicious activities; Reports suggest upto 85% of the mobile phones used are in Android platform [1]. At the least, a smartphone user uses a minimum of 12 applications, which arises the question, "Is your mobile safe?". This paper focuses on the said problem and provides an insight about some common types of attacks that use the vulnerability in applications and some defense methods and techniques that could be followed to prevent them.**

***Index Terms*—Android, smartphones, safe, attacks, defenses.**

I. Introduction

TECHNOLOGY is day-by-day getting really advanced and it is becoming an essential part of life. Compared to the mobile phones, which mainly provides telephony functions, Smartphones are handheld communications devices that support multimedia communications and applications for work and entertainment. Due to this fast growing functionality, the rate of usage at which updating traditional mobile phones to smartphones is tremendous. As per reports of statista portal, it almost crossed more than 100 billion mobile applications had been downloaded from the Apple App Store and the number of free mobile apps downloads crossed more than 92 billion [1].

The expeditious growth of the global smartphone market in the upcoming years will also be escalated by the increasing business use of smart- phones. Besides the basic traditional corporate-liable model, the new BYOD (bring your own device) model is gaining much acceptance in enterprises throughout the world at present. According to these studies, International Data Corporation believes that in 2013, 132.3 million were used as employee-liable and 61.4 million smartphones were used as corporate-liable devices [4]. Most popular mobile properties are mainly being accessed using mobile apps instead of mobile browsers. Some of the popular examples are mobile social-networking properties, led by Facebook with 727 million monthly active mobile-only users [4]. Other growing market is mobile retail via shopping apps, and also as well as mobile gaming and other possibilities of app monetization.

One of the major distinct features of smartphones is that they give provision for the users to install and run third party application programs which are usually in generalized term called as apps. According to different standard app reports all over the world, the usage of android apps is more when compared with the other mobile operating systems and also android gives easy provision for the users to develop and run their own apps as it is open platform [1]. This openness gave the malware writers easy directions to introduce the malware using mobile applications and extract the user sensitive information.

II. Vulnerability of Smart Phones

Smart phones are vulnerable to security attacks due to many factors. Some of those are:

- Users tend to store a lot of personal data in their smart phones, particularly as many people these days prefer to use online banking services for many financial purposes and choose the feature of saving their details on the phone itself; such data is sensitive [3]. Hackers gather such data from the smart phone to use it to their own advantage of gaining financially in a substantial manner, thus making a smart phone remunerative [2].
- Most of the smart phones used are developed on the Android platform; and with the platform that encourages open-source kernel, malware writers have a the chance to gain a better understanding of the platform. Googles marketing strategy, which encourages the development of third-party applications and publishing them has always been easy to gain a profitable market share [5]. Thus, hackers are presented with an opportunity to create and publish malware of their choice. And, as the never ending usage of smart phones by owners increases, so does the installation of malware which cannot be controlled very easily.
- Most smart phone users are not aware of the fact that their phone is a handheld computer that is vulnerable to any kind of cyber attacks [2]. They assume that their smart phones are just mobile phones that have many applications installed for communication and entertainment purpose [2]. Hence, there is not much attention that is paid to security measures.

Additionally, the origin of hardware and operating system of the smart phones has had the malware writers less constrained about the implementation of their actions. Besides, it is always easy to migrate a computers malware to any of the smartphone platforms.

III. Malware-Behavior and Threats

Malicious attack behavior, remote control behavior, and propagation behavior have always been characterizing mobile malwares [7]. Attack behavior concerns about how the mobile malware will exploit the infected mobile device further by infecting all the other victims devices using different communication channels, e.g. Bluetooth [7]. Remote control

Fig. 1. How safe is your Mobile App?

behavior is about how the mobile malware untilises a remote server to exploit a mobile device further after infecting it [7]. Propagation behavior is about the how malware can be transmitted to the victims [7].

A malware would try to acquire access to the data stored in the devices, and meddle with the functionality of the device, and possibly open up more security vulnerabilities like enabling unauthorized remote access to the hacker. There are many threats which can be launched using malware, which have been listed in the next subsection.

A. Attacks

The most typical attacks due to malware include the following,

- **Mobile application permission leakage attacks:** The Mobile application permission leakage attacks are of three types: Confused deputy attacks, Intent Spoofing and Permission collusion [6]. Confused deputy attacks are completely depending on misconfigured mobile applications. Intent spoofing is similar form of confused deputy attack which effects the applications that are not meant to communicate with other applications [6]. Collusion attacks are the attacks which uses overt and covert channels and aggregates the permissions from different mobile applications and releases user mobile sensitive data [6]. Collusion attacks are quite difficult to detect and which causes a great deal of research in the mobile applications.
- **Spyware Attacks:** Spyware is malware that conveniently collects information from an infected device. A user stores a lot of information on a smart phone which attracts the hackers towards it. Besides, there are many channels that can be used in smart phones to collect information. For instance, an application that shows the weather conditions would have a permission to send the location data to servers, which can be used by the hacker to acquire the location of that user in a malicious manner. Sometimes, when an application might seem legitimate in most senses, the permission settings in a users phone might not be secure enough to prevent such abuse of a permission given.
- **Phishing attacks:** Malware needs to have a database of fake URLs that are capable of taking a users personal information like credit card details, and any other personal information that can be misused as the websites have been cleverly masquerad as trusted websites. Studies prove that 25 percent of attacks use such techniques [8]. As this type of attack do not have a requirement of attacking the user directly in any manner due to its platform-independent nature, they are mostly applicable to smart phones. There are numerous reasons for a hacker to prefer this attack. Some of which are,
  - The smaller screen of a mobile device (in this case, smart phone when compared to a personal computer) tends to enhance the chances of disguising the trust sign which any user would rely on to make a decision of submitting credentials, for instance, if a site is enabled by Secure Sockets Layer.
  - A smart phone provides a large variety of channels to use phishing attack on, due to wide scale of applications that are used. These channels include short message service, or any other messenger applications.
  - It is facile to mask the infected application as a legitimate application and cleverly distribute them in the market for usage.
  - Many users are not aware of the fact that a smart phone gives the same risk as any other personal computer and tend to trust it more than a computer which obviously makes the computers work easier.
- **Diallerware Attacks:** A hacker can cause a financial loss to a smartphone user by diallerware attacks, which send premium-rate SMS without a user being aware of it [10]. The premium rate SMS service were created to provide value-added services like news and stock quotations periodically with the price of it being charged to the users phone bill. This can be used by the hacker to financially deteriorate the user without them being aware of it.
- **Worm-Based Attacks:** A worm has the capability to compromise on the security of smartphones [10]. Besides, its nature of duplicating itself and propagating

from one device to another without the users notice helps the case [10]. And as network function virtualisation has been introduced lately in the next generation of mobile phones, worm based attacks have a chance of increasing exponentially.

- **Botnets:** A set of zombie devices that are remotely controlled by a hacker when infected by malware is called a botnet [10]. When there are many mobile devices in the network, it is called a botnet [10]. They impose serious security threats to the Internet and most of them would be likely used in any organized crime, to launch attacks and gain profit financially.
- **Financial Malware Attacks:** This attack aims at stealing credentials from a smartphone by using buffer-overflow techniques or man-in-the-middle attacks on financial applications that are run by the user [2]. As we have established earlier, a smartphone is equally prone to risks as much as a computer is. Financial malware can come in many forms, for instance, it could just be a key-logger application which collects credit card numbers, or in a more sophisticated format, it could be an application that impersonates a real banking application that can launch man-in-the-middle attacks when a user is performing a bank transaction.

B. Malicious activities through Mobile Apps

Some of the ways where malicious activities can be introduced through apps are as follows:

i. Most of the app developers tend to request permissions which are irrelevant to the app, this makes the easy provision for malware writers to introduce their malicious activities.
ii. If two apps were developed by the same developer then there may be chance of collusion attacks where in the case of user ID are shared using API calls which is more dangerous.

IV. Defense Mechanisms

There are different strategies to defend against malware, some of which have been listed below:

1) Proactive detection can be done by using tools or softwares.
2) Creating honeypots so that can catch hold of malware writers easily.
3) Updating the applications within short span everytime.
4) System cleanup everyday.
5) Using most trusted applications by verifying the signature of the used applications.

A. Preventive Measures

Listed below are a few preventive measures that can be taken in order to avoid malware attacks.

- **Application Developers:** Most of the malware attacks are introduced using mobile applications. The application developers should follow the secured policies strictly by not giving any sort of the loopholes to the malware attackers. The Android consists of about 135 permissions out of which by different researches at about 30 permissions are considered as malicious and Android itself has categorized 23 permissions as the most dangerous permissions, so developers should restrict using these malicious, dangerous permissions in their application so that scope of introducing the malware decreases.
- **Smartphone users:** Smartphone users should strictly restrict app installation from untrusted mobile markets or websites. Most of the malware have been introduced by Chinese, Russian developers, so when any smartphone user who is installing an app should check the developers by whom app is offered by, reviews should be checked, users shouldn't blindly accept all the permissions, if the user feels that there are some dangerous permissions which are not required for the app they should be disabled, even the app runs by disabling some permission which can be done after installation.
- **Mobile market administrators:** Mobile market administrators should follow strict policies to ensure that mobile market is secure and highly trusted mobile market. If an app is found suspicious that should be removed and developer should be blocked. Apart from different scanners like bouncer which scans to find malicious activities, it is necessary to provide few more scanners that enhances the usage of apps through scanners.

B. Detection Techniques

Most of the malware can be detected in either of two ways, i.e., by using signature based detection or anamoly based detection. Signature-based detection solely concentrates on detection through signatures, it has some limitations like if the particular signature of app has not been found in the database detection fails.

Anamoly-based detection is done based on the behavior of the system, it mainly checks whether there are any inconsistencies in the behavior. This anamoly-based detection and signature-based detection are basically techniques which are usually comes under network based detection. Detection will also done in client side which is called as client side detection. Client side detection is again classified into static client detection and dynamic client detection. Static and dynamic client detection performs detection in terms of signature based detection and anamoly based detection.

V. Conclusion

In this paper, we presented a summarized view on different type of attacks by which a smartphones' vulnerability is exploited. Most smartphone users are dependent on using different apps for their daily-usage. For all e-transactions, the respective merchants are providing their own applications, as Android is an open platform and it is not secure enough to use untrusted apps. In near future almost every transaction can be done through mobile applications, for instance, paytm. By summarizing the attacks, that would give a smartphone user an idea about the types of attacks which can be introduced in different ways into an application to make it malicious. By this, we conclude that every user should have awareness if the apps used by the user are safe enough or not.

REFERENCES

[1] Portal, Statistics. "Number of monthly active Facebook users worldwide as of 1st quarter 2015 (in millions)." Luettavissa: http://www. statista. com/statistics/264810/number-ofmonthly-active-facebook-users-worldwide/. Luettu 26 (2015).

[2] Kulkarni, Shakuntala P., and Sachin Bojewar. "Vulnerabilities of Smart Phones." (2015).

[3] Kang, Joon-Myung, Sin-seok Seo, and James Won-Ki Hong. "Usage pattern analysis of smartphones." Network Operations and Management Symposium (APNOMS), 2011 13th Asia-Pacific. IEEE, 2011.

[4] Ballagas, Rafael, et al. "Byod: Bring your own device." Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp. Vol. 2004. 2004.

[5] Rekanar, Kaavya. "Text Classification of Legitimate and Rogue online Privacy Policies: Manual Analysis and a Machine Learning Experimental Approach." (2016).

[6] M.Kireet, Dr.Meda Sreenivasa Rao. Investigation of Collusion Attack Detection in Android Smartphones. International Journal of Computer Science and Information Security, (IJCSIS) Vol. 14, No. 6, June 2016.

[7] D. Guo, A. Sui, and T. Guo, A Behavior Analysis Based Mobile Malware Defense System, Proc. ICSPCS, pp. 16, 2012.

[8] Garera, Sujata, et al. "A framework for detection and measurement of phishing attacks." Proceedings of the 2007 ACM workshop on Recurring malcode. ACM, 2007.

[9] Mylonas, Alexios, et al. "Smartphone security evaluation The malware attack case." Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on. IEEE, 2011.

[10] He, Daojing, Sammy Chan, and Mohsen Guizani. "Mobile application security: malware threats and defenses." IEEE Wireless Communications 22.1 (2015): 138-144.