SMART PHONE SECURITY: WHAT MAKES SMART PHONES SO RESISTANT TO BUGS COMPARE TO COMPUTERS

Chinnu rajan

Assistant Professor
Balaji Institute of Telecom & Management, pune

ABSTRACT

These days, the use of cell phones and their applications have gotten quickly famous in individuals' every day life. In the course of the most recent decade, accessibility of versatile cash administrations such as mobile- payment systems and application markets have fundamentally expanded because of the various types of applications and availability given by cell phones, for example, 3G, 4G, GPRS, and Wi-Fi, and so on. In a similar pattern, the quantity of vulnerabilities focusing on these administrations and correspondence systems has raised also.

Hence, cell phones have become perfect objective gadgets for vindictive software engineers. With expanding the quantity of vulnerabilities and assaults, there has been a relating climb of the security countermeasures introduced by the analysts. Because of these reasons, security of the payment system is one of the most significant issues in portable mobile- payment systems . In this overview, we plan to give a thorough and organized outline of the exploration on security answers for cell phone gadgets. This overview surveys the cutting edge on security arrangements, dangers, and vulnerabilities .We layout a few countermeasures planned for ensuring cell phones against these gatherings of assaults, in light of the location rules, information assortments and working frameworks, particularly concentrating on open source applications.

With this classification, we need to give a simple comprehension to clients and scientists to improve their insight about the security and protection of cell phones.

Keywords:Mobile security, malware,malicious attacks

I. INTRODUCTION

These days smartphones are widely used and popular than personal computers and offers lots of connection 3G,4G,wi-fi,GPS,LTE,NFC and bluetooth. Now a days peoples are more familiar with different smartphones . But few are familiar with mobile Operating Systems and their securities. There fore Android Operating Systems are more popular than the desktop operating systems such as Windows,Mac,Unix,and Linux etc. So smartphone usage is more than desktop usage.

In this paper i tried to cover Existing Literature about smartphones, describes different types of Malware (Viruses) software attacks or threats, some existing security against viruses for smart phones ,some research areas about malware detection for cyber security and also discussing several factors that makes smartphones much safer for sharing or transfer personal information than your computer.

Smartphones are more safer to use , when we are compare it with personal computers. While doing your computations through PC or smartphones, both are you need to protect from cyber attacks. For that you have to run your virus scan daily or to keep your security software up to date. In your smartphones quickly scan for viruses and can remove any security threats.

Globally the popularity of PCs is on downword Trend, because more peoples are using smartphones are their computing devices.

II. SMARTPHONE OPERATING SYSTEMS

Smartphones are having different features depends on what technology they have . Features are Camera, fingerprint, face recognition, sensors, NFC etc. Operating system is controlling the features using different technology .And also controlling security, multitasking etc. Smartphones are using different operating systems such as Android, Apple Ios, Microsoft Windows phone, Blackberry and others. Other third party applications that are available for smartphones through online.

APP Store (Market)

Application Store contains different applications , user can browse or purchase the application through the stores.(Eg: Google Play store (Android),Apple store(iOS) AND Microsoft store).
All application stores are checking the applications by high-level anti - malware before releasing them.There fore we can say possibility of affecting bugs on smartphones are very less as compared to personal computers. Currently companies are using bugs detection techniques are signature based and machine learning (behaviour) techniques. But these techniques are still do not find unknown viruses.

SYSTEM ARCHITECTURE

Android

Android is open source operating system created by Google,based on the Linux Kernel and primarily designed for touch screen devices.

Android operating system contains 4 layers.

- Linux Kernel
- Libraries
- JAVA API Framework
- System Applications

Linux Kernel

It is managing virtual memory, physical device drivers, network management, and power management. These are core system services.

Libraries

This layer consist of open GL/ES, audio manager, open source web browser engine webkit, SQLite database, which is useful storage for saving and sharing data .SSL Libraries provides internet security.

JAVA API Frame work

This layer uses JAVA Classes to provide services for application. This application frame work provides the key services, activity manager, content providers, resource manager, notification manager and view systems.

System Applications

Android has a set of core applications for contacts, SMS messaging, Email, Calenders, internet browsing. System application operate for end users and which provides key capabilities which developers can have access from their own application.

SECURITY

The Google has introduced various security layers for android operating systems. Five key security features of Android as follows.

1. Security at the operating system level (Linux Kernel)

Linux kernel is having set of security measures. It gives user based permission model in interprocess communication, process isolation and its clearing any unwanted insecure parts of kernel. It also deny multiple system users from accessing each other's resources.

2. Mandatory application SandBox

This feature used for a user-based protection. And to create an "Application Sandbox" which assigns a unique user ID to each app, and each one can run its own process. It means that if a application infects by virus for a user, that person gives application permission then only it infects to other person's phone. This permission need to collect data . It can't be execute files in SD card till you get permissions. In personal computers, if you download a software with virus, it can keep on harming your personal computer even after you delete it.There fore in personal computer viruses can infect other files also with out confined to their own " Eco Systems".

3. Secure Inter-process Communication

Android is using Linux kernel to perform each application at the process level. It does not allow applications to interact with the other applications and allows them only some limited accesses to the Android OS.

4. Application signing

This is a key feature which provides the user permission-based access control and it provides a list of permissions on the first page of installation package (APK) .After running on the device the intended app will access them.

5. Application-defined and user-granted permissions

It gives a set of permissions on file systems. Each application has its own files .Files generated by one application cannot be able to read or changed by another one (i.e., if an company wanted to share data between some of its own Android apps, it can use "Content Providers" via custom permissions to share the data). Permission prevents any other apps on the device from accessing the app"s data unless access was specifically requested & granted to the intended apps.
Once a custom permission is set, only apps which were granted the custom permission can initiate interprocess communication with the protected app).

III. MALICIOUS ATTACKS

Now a days, Smartphone users are downloading their application from play store for different purposes such as social networking, play new games, photography. Generally they do not think about the application, whether it is affected by viruses or not. They are installing the application in their devices and activate the applications. Because of these reasons number of infected smartphones are increasing year by year. In any case, the Android has some fundamental systems to control .The authorizations of applications and the most significant issue is that the wide number of unpredicted (or obscure) assaults are focusing on shrewd contraptions, for instance, if a malware application plays a job like a genuine application with consistent authorizations and conceals a few malignant exercises in front of its, at that point how the OS can distinguish regardless of whether it is malware or not. Clearly, it is basic that the clients uses an incredible enemy of malware (Anti-Malware) to moderate those assaults. Further, in view of the most recent reports by the F-Secure and Kaspersky security groups which delineated.

Software security issues are categorised in to three .

- Malicious Software
- Vulnerabilities
- Attacks or Threads

1. Malicious Application

Mobile Malicious Application (MMA) is a covered up malware that can work out of sight of victim's cell phone totally vague to the client, and moreover, it is accessible to execute or associate with different systems for getting new guidelines. The MMA likewise can control the victim"s gadget and lead to increasing a few outcomes. For instance, a MMA can make an impression on the particular number or release the client area without its information . In other words, the current adaptation of the MMAs is getting such a great amount of refined with malware that can run in the front of genuine applications, with no doubts to the clients and anti-malware too, at that point they can play out some stunt exercises leveled out of malevolent clients. The up and coming age of MMAs is anticipated to be considerably increasingly shrewd, with botnet inclinations to control and commandeer victim"s gadgets.

Malware

Malware is a malicious software, used to access user information from their devices. And Anti-malware is used to predict their activities. Researchers has catagorised malware application in to 4 types.

(a) Virus

Virus is a malicious application that can acts itself and its actions can affect to other applications. In order to duplicate the infection in victim's device, the infected application must be sent to the objective device and performed by its client . For example, in 2016, a particular infection has been found by check point group that contaminated more than 85 million Android cell phones far and wide. It was called "HummingBad".

(b) Spyware

Spyware is a virus which is used to find the device for controlling the locations, contacts, calls, texting and emails. In some cases, it can send such data to somewhere else by means of accessible systems (or email, SMS, etc.) and take control for a device without the user's permission. For instance, Citizen Lab has found another risky sort of spyware in 2016, which was named "Surveillance" in Android and "Pegasus" in iOS. Spyware effectively allows hackers to take total control of devices such as collecting emails, monitoring calls and messages.

(c) Trojan

Trojan is a sort of malware that gives unapproved access to interactions of the clients such as purchase transactions, premium rate calls, and so on in the foundation of the victim's devices. The objective of this malicious applications is transmitting under the front of genuine applications or files. For instance, in view of the most recent report discharged by Tencent security analysts on February 2017 ,they have revealed another financial Trojan which is named "Swearing". Further, this Trojan contaminated a wide spread of Android devices and took bank accreditations of their clients furthermore, other delicate data in China.

(d) Rootkit

Rootkit is a concealed procedure that can run in the foundation of victim's devices and construct some malignant defects by tainting the OS for malware authors. Practically, this malware attempts to disable firewalls and anti-malware or hides vindictive client space forms for installing Trojans .For example, Gooligan is a sort of Rootkits which has been recognized with a cheque Point on November 2016. In light of their specialized report, another assault crusade has penetrated the security of more than one million Google accounts. This malware can uncover messages, photographs, reports and other information from the victim's device. Moreover, it roots the tainted device and snaffles validation tokens which are required to capture information from Google Play, Google Drive, Gmail, Google Docs, Google Photos, G Suite, etc. The Gooligan conceivably has tainted Android devices on (Jelly Bean and KitKat) 4 and 5 (Lollipop), which it was included over 74% of devices in the market. About 57% of these devices were situated in Asia and about 9% are in Europe.

2. Attacks or threats

Attacks are interruptions or dangers that are made by vindictive developers and, moreover, they utilize distinctive helpless vectors in the objective OSes (or applications) to assume the responsibility for the tainted gadgets. These interruptions normally called attacks or threats, where they used to take responsibility for the infected devices by means of malware

applications or vulnerabilities out of sight of victim's cell phones. Regularly, they are made by malware writers for accomplishing access to delicate data without the user's information . There are four principle kinds of assaults including social engineering, phishing, MITM and mobile botnets.

(a) Social Engineering

It is a hidden trick, used to disclose the sensitive information, fraud or system's password etc. This idea is a sort of hacking and includes vindictively manhandling to acquire touchy data that can be applied for vindictive purposes. Some times, social engineers act as a sure and educated employee, for example, managers or enforcers. In case of smartphones social engineers take advantages from malicious advertising.

(b) Phishing

Phishing app is a type of malware which acts same as real app for stealing sensitive informations such as user name, password. Technically, these fake applications acts like a genuine application by taking on the appearance of a reliable application on the victim's device. The phishing applications can break the confidentiality of client contribution for capturing login confirmations. For example, it can create a fake mobile banking login screen to hack the user information.

(c) Man in the middle (MITM)

Hacker creates a new connection between target device and banking server. The attacker divide the direct connection in to two new connections by using various ways. The primary connection is between attacker and server, next connection is between victim's smartphone and hacker. This attack is one of the viable dangers in light of the property of the TCP and the HTTP protocols which are all Unicode or ASCII standard based. In this way, the MITM hackers can translate and modify the information streams while they are going through the objective system.

(d) Mobile Botnet

It is a group of infected smartphones ,which are controlled by a Botmaster with out knowledge of the user. Botmaster is the person who prevents the normal network traffic flow. For example, the Check Point scientists have found another strain of malware on the Google Play Store. This malware is classified "FalseGuide" which was covered up in more than 40 applications for directing games and, in expansion, the principal variant of this malware was shared on the Google Play in February 2017. The "FalseGuide" can create a quiet botnet out of the contaminated devices for adware or malicious purposes. For this situation, a few applications were controlled to arrive at in excess of 50,000 establishments and the number of tainted gadgets was anticipated to reach up to 2 million devices. Besides, the Check Point informed the Google security group about this malware and they rapidly expelled it from the Google Play. Toward the start of the April 2017, two new fake applications were shared on the Google Play including this malware and the Check Point informed the Google security group again.

3. Software vulnerabilities

In smartphone operating systems, vulnerabilities is a weakness that allow an attacker to break the security of smartphones. Technically, vulnerabilities is the meet of three bases: a device susceptibility or flaw, attacker ability to elicit the flaw, and accessibility of attacker to the flaw. There have been two purposes behind expanding vulnerabilities on Android and iOS cell phones. First one, the Android is the most well known OS around the globe, which is open-source programming and in addition, there are an assortment of security shortcomings in old variants of Android. Also, the majority of the Android clients do not care about refreshing new fixes of the OS which may improve the security of their cell phones. Secondly, the clients used to download applications from official application stores.

IV. SUGGESTIONS FOR FUTURE WORKS

In case of security and privacy, the smartphones users are unable to find the number of attacks on their devices. Further more how much cash vindictive applications may take from their accounts. The obligation of the specialists is that research about clarifying security issues and report to the clients. There are as yet countless vindictive assaults, that are focusing on cell phones increasingly more as referenced in Section III . As a result, the majority of the clients don't utilize premium portable security programming and their devices are uncovered as the perfect objective for malware creators.

Suggestion points are

- Before installing one application from store the user can easily identify whether it infected by virus or not.
- The specialists can examine about the procedure observing and discover a connection between application procedures and yield results in the counterfeit applications. What's more, it tends to be utilized for the highlights extraction in OSes to declare the clients about the hazard of broke down applications. Using new AI procedures for giving ongoing conduct investigation and distinguishing counterfeit applications .
- To identify the fake applications use machine learning techniques.
- Network monitoring can used, due to the malware applications misuse a system association for moving information to the hackers. For example, when the device is idle, and an application is utilizing a system association, at that point it can speculate to be a malware.
- Doing malware testing, we can use deep learning algorithms to give accuracy.
- To prevent unknown attacks, mobile softare companies have to provide more security mechanisms.

V. CONCLUSIONS

with the rapid use of smartphones and developing applications, with the features of sensors, and connections the amount of virus attacks are increasing. The people needs more awareness to reduce the bugs. In this paper i tried to cover how mobile phones can resist threats than laptops, discussed famous operating systems in mobile, software vulnerabilities,

and the attacks which causes the smartphones. Smartphone users can concentrate on the problems that affect on the smartphones.

VI. REFERENCES

[1] Milad Taleby Ahvanooey, Prof. Qianmu Li, Mahdi Rabbani, Ahmed Raza Rajput, "A Survey on smartphone security: Software Vulnerabilities, Malware, and Attack".

[2] Polla, M., F. Martinelli, and D. Sgandurra, (2013), "A Survey on Security for Mobile Devices," IEEE Commun. Surveys & Tutorials,

[3] Kaspersky Lab Threat Review for 2016, Retrieved September 5, 2017,http://usa.kaspersky.com/about-us/press-center/press-releases/2016Kaspersky_Lab_Threat_Review_for_2016_servers_for_sale_global_botnets_and_a_strong_focus_on_mobile

[4] R. Dhayal, & M. Poongodj, (2014), "Detecting Software Vulnerabilities in Android Using Static Analysis", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[5] W. Melicher, D. Kurilova,Sean M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. Faith Cranor, Michelle L. Mazurek, (2016) , Usability and Security of Text Passwords on Mobile Devices, CHI"16, May 07-12, 2016, San Jose, CA, USA,

[6] Wikipedia

