I J C T A, 9(41) 2016, pp. 823-831 ISSN: 0974-5572

ANALYSIS OF SECURITY THREATS IN MOBILE USING CASE STUDY OF ANDROID OPERATING SYSTEM

Priyal Chotwani[1], Yash Anand[1], Vikas Deep[2] and Naveen Garg[2]

Abstract:Smart phones are becoming more and more famous due to the increasing power of processing, personal nature and mobility feature. Android is one of the most famous and completely customizable open source mobile platforms. It comes with a full software stack. One of the many reasons behind the rapid growth in vast usage of smart phones is their capability of providing users with third-party applications. Android offers uncountable applications through application markets like play stores and users can readily install these applications. However, all these aspects and the rapid growth of usage of android also draw our attention towards the security issues in android and make it a serious concern. Here, in this paper, we start with an introduction of the smart phones and the threats which are present in android operating system. We have discussed about these threats and malicious software in detail to work better on the security of android. We also present the android architecture and the architecture of security provided in android. We also mention about the improvements which were suggested for the basic Android security model. We also present certain suggestions for android users so that they can be aware and use their smart phones wisely to prevent themselves from any threats or malwares and put into effect the security strengthening for Android which can be widely used by the vast population...

Key Words: *Kernel, GPS, Malwares;*

I. INTRODUCTION

In older days the main purpose of mobiles used to be calling and texting each other. Mobile phones were only a better communication medium than letters. As mobile computing technology is developing things have changed as well. Unlike before, mobiles have many different features which are common to a modern computer, albeit primary role of mobile still remains communicating with each other via texts or calls but it is not enough for us anymore. Now, features like high screen resolution, camera of high quality or high speed of multi-core processors also contribute in the roles, which mobile phones play. Not only this, it also provides users with remarkable computing facilities like high storage capacity, locating places, GPS etc.

In addition, to a high speed and availability of Internet along with much low prices it is a usual thing to remain connected with internet all the time. In this high technology world android are becoming popular and in fact now it can be called equivalent to a computer. It is believed by International Data Corporation that android is going to maintain its position in market of mobile devices until the end of this year [13].

[1] *Student, Department of Information Technology, Amity University Uttar Pradesh, Noida, India,*
Email: priya.remastic@gmail.com, y.anand2407@gmail.com
2. Asst Professor, Department of Information Technology, Amity University Uttar Pradesh, Noida, India,
Email: vikasdeep8@gmail.com, er.gargnaveen@gmail.com

Android gives a platform to application for executing in cell phones. Kernel of android is comparable with UNIX operating system kernel that is utilized for its gadget drivers working, memory administration undertakings, and systems administration errands. Second level contains android local libraries which are joined by means of java local interface. There is an application layer which provides different applications, for example, web programs, email and so forth [14]. Applications in android are composed in java. Such design helps the engineers to create different android applications.

There are many services like online banking offered by smart phones which have become a part of everyone's life. A wide population is now using the Internet through their smart phones and tablets. There are various Application markets like the official Google play store which provide the users many different applications with a wide variety of functions [15].

The frequent and wide usage of android has raised the concern of security in the smart phones [2]. The various applications and open source nature of the operating system of android has allowed more malwares to attack the android sophisticatedly [16].

The most important thing for the security of smart phones is the capacity to have a safe and private communication irrespective of whether it is done via texts or voice calls. However this is not the only concern which makes us completely protected. Some important primary concerns are also the ability to securely remove and store data in a phone or to keep a user's location private [17]. Out of the above concerns, storage of data securely on the phone is currently the only choice which is provided in the Android Operating System.

In this paper we have presented an overview of the android architecture, security threats and architecture of security in smart phones with the brief detailing of the points mentioned, further we have covered the taxonomy of the threats in android framework after mentioning more about security requirements in android. Further there are few points mentioned about the security mechanisms applicable in android [18]. We have concluded the paper by mentioning about the end user where the emphasis is put on the user's responsibility and their awareness towards the security of their data.

II. LITERATURE SURVEY

Android has turned into the most well-known open source gadget for clients. It comprises of various implicit applications. Its design is made out of various yet associating layers. The lowest layer in the Android's engineering is the Linux Kernel that contains display drivers, camera drivers associatively known as hardware drivers and performs functionalities like memory administration, process administration and power administration. This layer is modified to incorporate an Android specific component called Binder, which is in charge of performing communication among different application segments [1].

The weakest component of mobile security is human as humans usually accept that everything will work according to how it is meant to be, relying on the default settings of the device without even consulting the specialized manuals provided by designers for the security of data [6].

Therefore, the responsibility of the hardware suppliers and the designers increases to maintain the device's security and keep a check on its content. Designers therefore can minimize the shortcomings of the device by adding security administrations in the device.

The problem of mobile security is a bigger issue for home environment than seen at any other place. The issue of cyber security is additionally a risk to versatile gadgets like tablets [19]. There are electronic

devices which are used at home on a daily basis and fulfill all our needs as intense as a computer, from cell phones, video games and auto route frameworks. While these gadgets are useful and provide more features, they likewise present new dangers.

For instance, an attacker may attack the device with a virus, to get all the information that is stored in the device. These actions affect the personal information, and also have dangerous consequences if corporate information were stored in the smart device [20].

The utilization of cell phones in medicinal services is likewise more regular nowadays, for example, in versatile wellbeing [21]. A typical example is having a medical gadget associated with the home, which is fit for sending information remotely to healing facilities and other significant places. The vast majority of the producers of these gadgets don't put much attention in attempting to ensure that the gadgets are secure [7]. If these gadgets are traded off not just will the data and security of the client of the gadget be bargained, yet the aggressor can even alter the settings of the gadgets, which could result into hurtful and harmful outcomes. It has been demonstrated that it is conceivable to hack and read the points of interest of information put away in the gadget, for example, names and therapeutic information without having direct access to the gadgets basically by standing close-by [8].

It is seen in the Juniper Networks report that 76 % of users rely upon their cell phones to access their most private data, for example, medical data via internet. This issue is of greater concern for the individuals who likewise utilize their personal mobile devices for business errands [22].

89% business clients report that they use their cell phone for trade purposes [23].

Individuals could download malware to their devices unknowingly or fall prey to "man-in-the-center" assaults and attackers usually take the advantage of such situation by catching and gathering sensitive data for pernicious and harmful use. In 2011, numerous Android applications were expelled from the Android Market because it was found that they contained malware [24].

III. Security Architecture in Android

The aim of the designer is to provide the user with the fundamentals related to the security concepts used in Android applications. These concepts aim to provide:

- It is checked that the personal data of a user in the device remains private
- Resources of the system remain private and secure

For achieving the goals which were previously stated, the Android operating system provides various levels of security. One of the models which were given by A. Gunasekera in book Android Apps Security is as follows [5]:

3.1 Permissions

Various applications require many types of allowance to use device component. However, who chooses whether to concede or refuse access? Android permits end client to play out this last endorsement process. It is important to remember that the consent should be given at time of installation.

3.2 Application Code Signing

At the point when an application is introduced, android working frameworks play out the testament check. Any application which keeps running on android working framework should be signed however utilization of affirmation power to sign the certificate is not required and application just need self-

marked testament. Android utilizes the declaration of individual engineers to distinguish them and set up trust connections among different applications running in working framework and it doesn't control any code.

3.3 Security solution proposed by Shabtai et al. is as follows

Application-Defined and User Granted Authorizations Android utilizes a required consent model. At the point when an application needs to utilize certain administrations, this must be plainly expressed in the show document. This implies upon establishment the client will be told which prerequisites are important for that specific application. With respect to, Android does not have a different authorization that plainly determines the utilization of this convention. Rather everything is gathered into one worldwide authorization that permits allowance to the Internet. Moreover there has been much exertion in looking into the authorization model and over-special applications that could prompt huge security issues and information robbery. Regardless of the possibility that the clients pay consideration on these notices, it is questionable whether non-technophile clients are adequately acquainted with the displayed terms, or the subsequent results.

IV. TAXONOMY OF THREATS TO THE ANDROID FRAMEWORK

Following are threats which come in user's device when he/she download, install, and run software that contain illegal codes. These attacks become possible since android applications aren't seen properly prior to make them available for download by user. Attacker can have access to user's private data, send untrue service texts, remove user's essential data, install other harmful applications like Worms or Botnet, through the attacks mentioned below, these can also prove to be a method for committing many cybercrimes.

Figure 1: Cyber Security [10]

4.1 Malwares (Virus, worms, Trojan horse)

Virus is harmful code that attaches itself to a file and come into action when that file execute. Also while executing they may replicate themselves and harm other applications as well. Worms also replicate itself just like virus and spread harmful code but unlike virus they do not need to execute an application to spread their code. Caiber is a worm that spreads in the device through Bluetooth links.Trojan horse is a malware which does not replicate itself like virus or worms, instead of replicating they pretend to do some useful task and gain control over the device's functionalities. The first Trojan horse reported in android was Fake Player. It was reported that this malware was a fake media player icon and was the reason behind sending messages without user's consent. In 2011 a malware known as droid dream was reported. The Trojan gained root allowance to Google Android mobile devices to access identification

data for the phone. Once the phone is infected, it could also install some more harmful programs without the user's knowledge [3].

Other harmful softwares are:

- Malware is harmful software whose work is to cause damage to all the information or cause data theft or gain allowance to the features of device. Therefore, a malware is made for the purpose of causing arm. Term malware includes all the type of malicious software for example viruses, Trojans, Worms etc. Following are the types of malware:
- Trojan is software, which causes harm to the user after getting activated.
- Worm is a harmful program which replicates itself.
- Spyware is a malware whose main concern is to get allowance to private data from a device.
- Adware is a program in which advertisements are shown while various illegal applications are running behind it.
- Ransom ware is software which locks the user's device and then forces the user to pay to unlock his device.
- Charge ware is a program that charges users without any clear message.

4.2 Botnet

This malware is responsible for spam delivery, attacks and personal information theft. This attack strategy is made in order to use the power of computers in order to commit various cybercrimes such as sending spam mail. First malware of this category was discovered in Dec 2011 called as Geinimi. It collects all the information in the device and transfers it to a remote server.

4.3 Advanced persistent threat (APT)

APT is a cyberattack launched by a group of intelligent and trained attackers. APT is also called as targeted threats as they target on enterprises and business organizations. Such attacks mostly target at getting access to the implicit storage to cause valuable data and business secrets theft. Security methods also fail to stop such attacks.

The national and international banks have reported in a recent survey that enterprise of around twenty respondents have already been associated by APT

4.4 Root Kit

It is a dangerous application which has the permission to run in a privileged mode. It hides itself from the user by changing functions of operating system. Recent research indicates that this attack strategy in a device can be proved as an evolving threat to the mobile security. Droid Dream is an example of malware which uses this root privileges. The security system that has no effect on this malware is permission system. Designers are trying to prevent such attacks.

V. SECURITY MECHANISMS APPLICABLE TO ANDROID

There are many ways of protecting mobile phones from the threats and malwares which have been listed in the above sections. Some of them are listed below which have been taken from the Google Android [4]:

Table 1 Comprehensive Security Measures

Threats	Description

Antimalware	Searches for presence of viruses, root kits, and many more of these malware in the device.
Intrusion	Detection or prevention systems which help to avoid cyber deceits by searching unusual or usual destructive behavior
Linux access control	(Acts like sandboxing) helps in preventing allowance to mobile features and applications.
Android permission access control	Prevent unneeded consents that aggressors can dangerously misuse.
Data or phone call Encryption	Prevents allowance to private information when mobile is not with right person.
Application certificate is checked	Can help users to avoid damage from unfaithful applications
Integrity checking	Verify device as well as application state to prevent offline interfering
Usage of locks which have hard passwords	Can ensure that data theft is prevented
Spam filters	Check for Spams
Remote management	Remotely manages device and help if there is any mobile theft.

VI. ALERTNESS OF END-USER

It is very important for the users to keep in mind some of the security measures in order to keep their devices and their data safe. There are few measures mentioned which should be kept in mind by the users [9]:

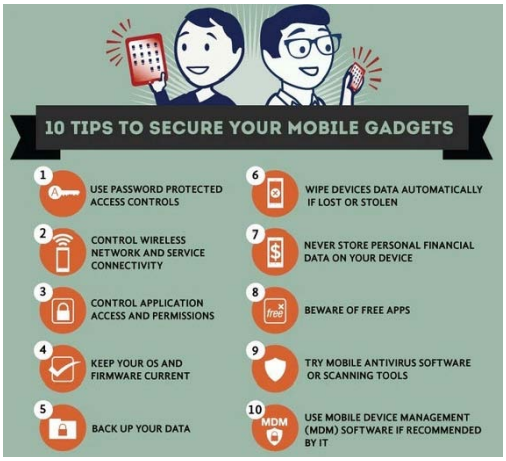

Figure4: Security measures for users [11]

5.1 Installation related measures:

- Anti-virus and anti-malware applications: It protects the phone from viruses and malwares respectively. These applications are found to be very helpful in protecting the devices from the harmful softwares. Therefore, it is recommended to allow the automatic update of these applications.
- Personal firewall: Direct attack or illegal allowance to the mobile phones is prevented.

- Applications from faithful sources having authentic contact data: As the present Android Market (Google Play) does not embrace an affirmation procedure for applications, it depends upon the users to ensure that they have installed faithful applications from faithful designers.
- Applications from the official designer: For instance, if you want to install Instagram then it should only be downloaded from Instagram Inc. It is necessary to check that these applications have high number of positive feedbacks and installations.
- Backup or restoration software: This software can be proved very helpful while retrieving or protecting any lost or stolen private data in mobile phone.

5.2 Ponits to ensure

- It should be checked that whether the permissions which are being asked during the installation time are really necessary. For instance, wallpaper application does not require the contact details.
- The software is always updated with the latest versions along with its security requirements.
- Not to install any application or program from any unknown sources. The option to deny the
- Installation of any application from an unknown source is provided in device's settings.

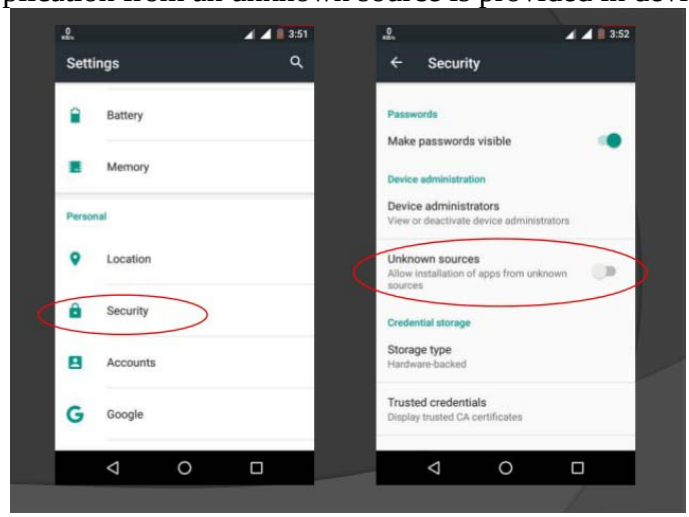

Figure 5: Security threats in android [12]

5.3 Sharing Data Concern:

- The private or sensitive information on the internet should not be seen through public wireless network which do not have any passwords.

5.4 Activities Occuring in Devices:

- Alertness to unusual and unacceptable behaviors in their devices should be noted and checked.

5.5 Using Internet Sites:

- Users should take care while clicking and opening links on social network sites. There are many harmful and dangerous links on social networks which are capable of spreading malware to the devices. For instance, users believe in such sites and they click such links without any doubt and fall prey to the malwares.

VII. CONCLUSION

This paper conclude that not just engineers and scientists can solve the problem of security in android, users are also responsible for our security by acting smartly and not getting trapped by the hackers. Also

I want to suggest that since now we are aware that hackers can enter into the android operating system, we can prevent it by keeping passwords which are hard to guess or even hard to remember by users. This could be thumbprints or retina. Sometimes by applying hard passwords to protect it from hackers, it also becomes difficult for the users to memorize it. This problem could be solved if the passwords can be applied in thumbprints or retina forms only.

REFERENCES

[1] Sheran A.Gunasekera,"Android Architecture", in Android Apps Security, Ed.New York: Apress, 2012

[2] S. Gunasekera, Android Apps Security, 1st ed. Berkely, CA, USA: Apress, 2012.

[3] K. Dunham, "Mobile Malware Attacks and Defense", Syngress Publishing, 2008.

[4] Google Android: A Comprehensive Security Assessment, co published by The IEEE computer And Reliability Societies, March/April 2010

[5] W. Enck, M. Ongtang, and P. McDaniel, "Understanding android security," IEEE Security and Privacy, vol. 7, no. 1, pp. 50–57, Jan. 2009.

[6] Juniper, "Juniper Networks 2011 Mobile Threats Report," Juniper Networks Mobile Threat Center (MTC), 2012.

[7] J. Blumberg, "Cyber security, Health Care, and Mobile Devices," in Dartmouth Now, 2011.

[8] Mobile Attacks and Defense, white paper co published by The IEEE computer and reliability societies, July/August 2011

[9] Image: Cyber Security, reference: blog.mass.gov

[10] Image: Security threats in android, reference: www.slideshare.net

[11] Chhikara, Pallavi, Gurpreet Singh Matharu, and Vikas Deep. "Towards OpenFlow based software defined networks." Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. IEEE, 2014.

[12] Aggarwal, Sahil Kumar, Vikas Deep, and Robin Singh. "Speculation of CMMI in agile methodology." Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[13] Priyanka Upadhyay, Rajesh Singh, Naveen Garg, Abhishek Singh,"Evaluating Seed Germination Monitoring System by Application of Wireless Sensor Networks: A Survey" in conference proc. Of 2nd International Conference on Computational Intelligence in Data Mining, ICCIDM 2015 published in Advances in Intelligent Systems and Computing 411, DOI 10.1007/978-81-322-2731-1_24 – Springer Journal pp. 259-266.

[14] ur Rahman, Munib, et al. "Implementation of ICT and Wireless Sensor Networks for Earthquake Alert and Disaster Management in Earthquake Prone Areas." Procedia Computer Science 85 (2016): 92-99.

[15] Tanwar, Rajneesh, et al. "Railway Reservation Verification by Aadhar Card." Procedia Computer Science 85 (2016): 970-975.

[16] Lal, Divya, et al. "Advanced Immediate Crime Reporting to Police in India." Procedia Computer Science 85 (2016): 543-549.

[17] ur Rahman, Munib, Vikas Deep, and Santosh Multhalli. "Centralized vulnerability database for organization specific automated vulnerabilities discovery and supervision." Research Advances in Integrated Navigation Systems (RAINS), International Conference on. IEEE, 2016.

[18] Prerit Datta, Namandeep Kaur, Naveen Garg,“Automatic Bus Fare Collection System in India” in conference proc. Of 2nd International Conference on Information Systems Design and Intelligent Applications, INDIA 2015, published in Advances in Intelligent Systems and Computing – Springer Journal pp.681-689.

[19] Chaudhary, Lalita, et al. "Business Modeling Using Agile." Information Systems Design and Intelligent Applications: Proceedings of Third International Conference INDIA 2016. Vol. 1. Springer, 2016.

[20] Chaudhary, Lalita, Vikas Deep, and Preeti Chawla. "Systematic Evaluation of Seed Germination Models: A Comparative Analysis." Information Systems Design and Intelligent Applications. Springer India, 2016. 59-65.

[21] Shweta Shukla, SnehaSonkar, Naveen Garg,“A Technique for Prevention of Derailing and Collision of Trains in India” in conference proc. Of 3rd International Conference on Information Systems Design and Intelligent Applications, INDIA 2016, published in Advances in Intelligent Systems and Computing 433, DOI 10.1007/978-81-322-2755-7_30Springer Journal pp. 291-296.

[22] Chawla, Preeti, et al. "Systematic overview of mobile virtualization platforms: Comparative analysis." Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015.

[23] Sharma, Anshul Kumar, Vikas Deep, and Naveen Garg. "An efficient way of articulation or suppression in agile methodologies." Confluence 2013: The Next Generation Information Technology Summit (4th International Conference). IET, 2013.

[24] Gurpreet Matharu, Priyanka Upadhyay, Naveen Garg,“Modeling Agility in Internet of Things(IoT) Architecture” in conference proc. Of 2nd International Conference on Information Systems Design and Intelligent Applications, INDIA 2015, published in in Advances in Intelligent Systems and Computing – Springer Journal pp. 779-786.