ISSN: 0975-766X
CODEN: IJPTFI
Available through Online *Review Article*
www.ijptonline.com

SURVEY ON MOBILE VULNERABILITY ISSUES AND BASIC SECURITY POLICIES

***Kaushik Roy and Ramya G.**
School of Information Technology and Engineering, VIT University, Vellore-632014, India.
Email: kroy.compsc@gmail.com

Received on 22-04-2016 *Accepted on 18-05-2016*

A. Abstract

In last few years mobile computing field has been emerged faster than the any other field of computing. In last decade we have introduced with smart phone, touch phone and they were not only used for calling someone. The experience was more than our previous expectations. But at the same time it has become threats for us sometime. Day by day the thin line difference between a PC and mobile device is becoming invisible.

Nowadays in an average a smart phone has web browsers, media player, camera, Bluetooth, Wi-Fi, GPS and may other applications. Because of insufficient access control strategies and absence of data on securing cell phones it is important to consider the difficulties of provisioning and overseeing security in cellular telephone situations.

From the network security view point there are four basic parameters, taken care about for a user's security; those are Authentication, Confidentiality, Integrity and Non-repudiation.

This review paper helps to understand all aspects of those four parameters and mainly focuses on the vulnerability issues of smart phone and how those can be reduced.

Keywords: Mobile Computing, Vulnerability Issues, Security Policies.

B. Introduction

In this lightning-fast modern world we need quick access of everything, literally it means everything. During our journey we are paying bills, sending money, buying products, checking our social networking sites, uploading photos, viewing map and road direction in an unknown place, booking railway/bus tickets , so basically its everything. All those become possible because of mobile computing and the mobile devices with high processing efficiency. Every day we use our smart phones as confidential data storage, synchronizing with email/social site, connected with online cloud or banking

account and others. From a commercial site called "ringtoindia.com" did a survey on the growth of overall mobile/smartphone users in India than the last years [4](Fig. 1).

It can also be observed that in the year 2013 the number of PC users was started decreasing gradually then the number of smartphone users.

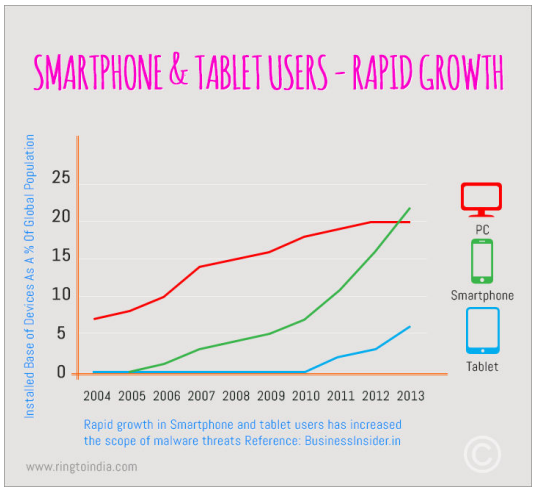


Fig. 1: Growth of smartphone users.

As we know "prevention is better than cure", we should take care about the security of our devices before not only we loseit, but also we lose everything with it. To understand the security policy we need to understand the vulnerability issues of our smart phones.The principle of security based on four principles- Authentication, Confidentiality, Integrity and Non-repudiation [1]. Let assume A is a sender and B is receiver. Now if A sends a packet to B and no one except B can read it is called as confidentiality. After receiving the packet if B wants to verify if indeed it has been sent by A, he can also do that, it is called as authentication. A and B want to ensure that no one can temper the content of the packet is known as integrity. If the content of the packet is something much classified information deal between A and B, non-repudiation ensure that A could not deny this fact that he himself sent that packet to B.

Security is an important fact to take care about the fact, that one can illegally access someone else's data/identity. As the number of different connectivity component increased for a smart phone, like GPRS, Bluetooth, infrared, Wi-Fi, GSM, it also increases the vulnerability [2].

Smartphones and feature phones may be considered as handheld PCs coordinated inside of a cell phone, however while most feature phones have the capacity to run applications in view of stages, for example, Java ME, a cell phone permits the client to introduce and run more propelled applications basedon a particular platform. Smartphones run complete

working framework programming giving a platform for application developers[3]. The powerful advantage of smartphones is based on the requirement/feature user can develop any application and also can customize the functionalities, specially for the android [5]. For example nowadays an apps can tell you the restaurants, ATMs, bus stops, railway station near to you, just in one click.

Clients own cell phone can be utilized to build profitability of an association. Users can get to corporate resources from their own particular cell phones. [6] However, presenting cell phones in the endeavor presents extra security challenges. Android gadgets may even serve as remote bases for assaults on other GSM supporters, however this is respected profoundly doubtful. A few new and understood danger situations apply for Android smartphones. These incorporate effortlessly conductible cash extortion, mechanical reconnaissance, corporate or military system invasion and even dissent of administration assaults on today's as of now vigorously stacked versatile system.

C. Literature Review

In their paper Rahul B. Mannade, Amol B. Bhande [7] has talked about around three most imperative parameters in mobile computation that are Communication, Mobility and Portability. Presently a day portable uses the remote innovation which accompanies littler lighter and less utilization of force however in the meantime it is truly difficult to execute than wired technology. Some major natural elements influences the association gave by remote innovation, in this way it is more mistake inclined, with lower transfer speeds and separation issues. Versatility, keeping up the nature of administrations while a gadget is being moved, changing areas, is additionally a state of concern. The versatility feature likewise manages address allocation, individual area based data and protection. The third imperative, portability accompanies the prerequisites sturdy, smooth configuration, convenient, little and light which disturbs the liberal methodology taken by creators before. The authors has likewise communicated their perspectives about how these circumstances can determined by utilizing mobile assets(like CPU, Cache, Memory) accurately, utilizing some exceptional strategies, for example, logging, consummating, pressure , compose back storing and so forth.

As the popularity on smart phones are increasing day by day, proportionally the security issues are also becoming a matter of concern. Soeung-Kon(Victor) Ko, Jung-Hoon Lee, Sung Woo Kim [8] did the first reported survey on the vulnerability and security issues of a smart phone. Later Srikanth Pullela [9] was focused on the network security and he concentrated on the principles of network security with more two parameters.

Legitimate and Accountability. Accountability infers that an element ought to be considered in charge of its own particular activities, where as Legitimate infers to identify a legitimate communication network or sender of any message. He clarified that if these factorsare maintained properly in a communicational network, specially when it is wireless, then it can be a maximum level of communication.

An itemized overview on Different sort of assaults on portable and the qualities of different sort of malware , Trojan stallion and malevolent records which can degenerate versatile information , has been finished by Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra [10]. The authors has additionally indicated a few courses by which those pitfalls can be evaded.

D. Vulnerabilities and Threats

Vulnerability and Threat are not the same. Vulnerability means the weakness of a system, or the risk to a system potentially, whereas threat means shaping the attack using the weakness of a system. In past few years the attack on mobile devices has been increasing like fire in forest. The biggest reason behind this is the Android OS. Android has no control on the developers and their built applications. There is no such malware scanning over the published apps, specially when it is on a third party website, at the same time a user can work as an admin of his system OS. Android was designed as a true open source, so it is also a open field for a hacker to embed some malware code inside a legitimate apps and republish it on his website [14](Fig. 2).

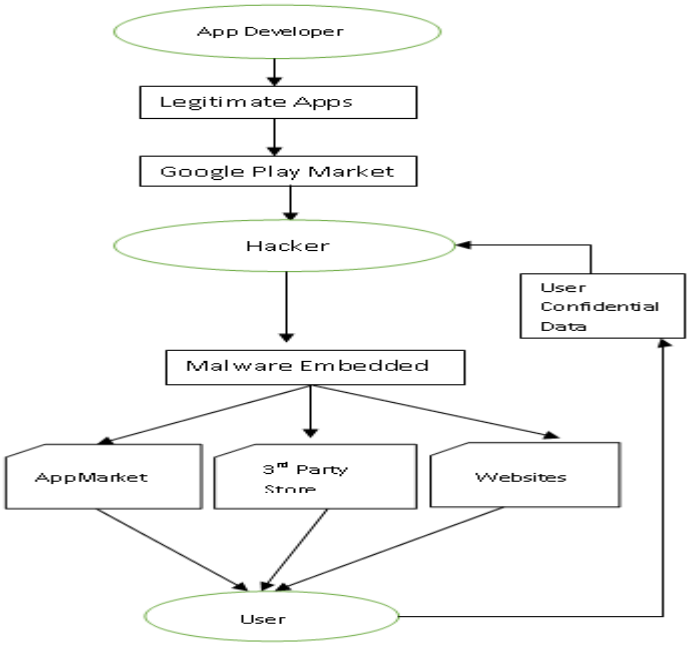
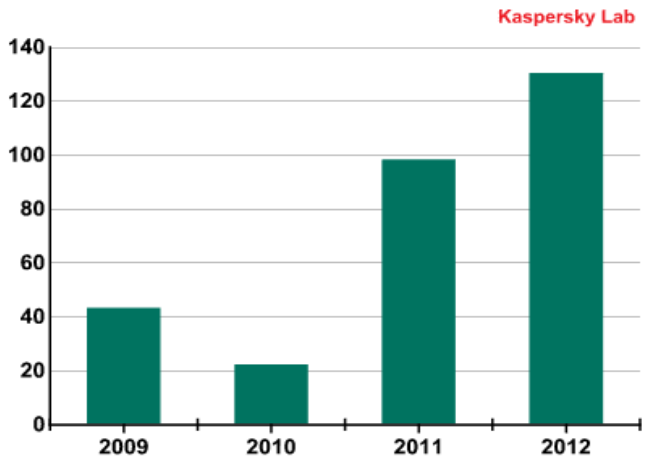
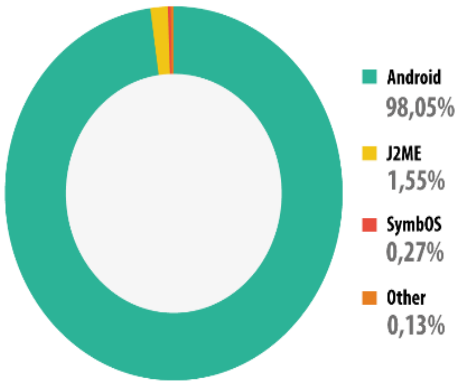


Fig. 2: Repackaging malware into legitimate app.

Initially connecting a mobile with PC required one intermediate software developed by the device manufacturer. That software actually took care about the contents that were being exchanged between PC and mobile. In Android smartphones one can directly connect his mobile device with PC simply with USB cable and it exposes all the contents of SD cards with read/write/modify/delete access. These type of issues in smartphones are making themselves more exposed for a malware attack. Whenever the PC is connected with smartphone, the malware can be automatically exchanged between them [15].There are a few apps which can abuse the administrations of another app without consent demand [16]. Any app on the android platform will get to gadget information simply like the GSM and SIM advertiser Ids without the authorization of the client. In last few years because of all those vulnerability issues the attack on mobile devices has been increased much more that previous. Kaspersky lab reports confirm that the attacks have been increased significantly on mobile devices after smartphones hiked the market (Fig. 3 (a))[17]. The lab report also confirmed that the Android is most suitable for this type of attacks for the hackers (Fig. 3(b))[17].



(a) Year wise Statistics



(b) OS wise Statistics

Fig. 3: Attack Statistics

The biggest question is that what we need to secure from the attacks or illegal access. The Table1 describes the details of security objects.

Table 1: Security Objectives.

Issues	Description
Confidentiality	It ensures who could access the device and who are not allowed
Integrity	Who is allowed to use the system resources(CPU, memory, Data) and who is not
Availability	It signifies that a resource is always available for that person/apps who was allowed to use it.

Next important point to note is that what are the current vulnerability issues exists with a smart phone. Those are described in the Table 2. The first three (V1-V3) vulnerability issues can be considered as internal issues of a smartphone, as it depend on the system architecture and resources. Rest of two are considered as the external issues, as they are mainly occurred because of network problem or connectivity reason.

Table 2: Vulnerability Issue.

Vulnerabilities	Description
V1. Implementation issue	Because of architectural design of device a malware can take its advantage.
V2. Incompatibility	If there is any incompatibility between two apps, or an apps and the OS itself; we need some intermediate apps to make them compatible with each other.
V3. User Unawareness	Installing apps from untrusted sources, Connecting with unprotected public Wi-Fi and websites, improper configuration with system resources (like- Bluetooth, Browser etc.), unaware of social attacks, lose the device somehow.
V4. Wireless Network	Blocking, modifying the data packets by packet sniffing and spoofing or eavesdropping.
V5. External Objects	There are several external objects for which vulnerability increases significantly, like- web server, AP, base station, PC etc.

As we have already discussed earlier that vulnerability and threats are not the same and vulnerability leads the threats. The following Table 3 has discussed the different threats according to their vulnerabilities. First four (T1-T4) are caused by attackers and rest four cases (T5-T8) are because of the unawares of a user.

Table 3: Threats.

Threats	Description	Vulnerability
T1. Malware	It can alter or expose confidential information, risk the availability by holding the system resources, also can use costly services(MMS, SMS, Data exchange)	V1 V3 V5
T2. Wireless Network Attack	By packet sniffing, eavesdropping, spoofing the packet content can be altered or observed.	V4
T3. DOS Attack	Attacks on the base station (device), wireless network, radio interface, web servers to make them unavailable to use for the user.	V4 V5
T4. Break-in	Gets the control over the device through code injection or flaw of code	V1
T5. Malfunction	An application may malfunction because of incompatibility between the platform and application.	V2 V3
T6. Phishing	User can expose his/her confidential information by accessing a phishing website or message phishing.	V3
T7. Loss	Lose the device itself	V3
T8. Platform interchange	A user can alter the internal platform configuration of his/her device(jail break for iPhone or rooting for Android)	V3

The next figure (Fig. 4) describes the statistical data of different types of threats and attacks from Kaspersky lab data [18].

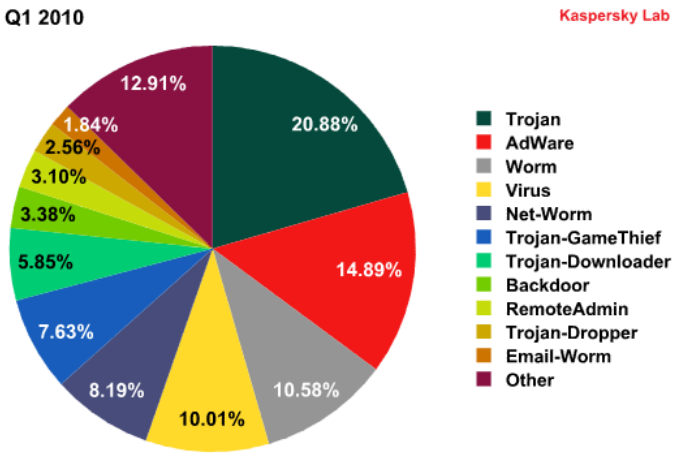


Fig. 4: Statistical Data of attacks and threats.

All types of attacks can be classified into three major categories [19] - Malware, Grayware and Spyware. Malware access the confidential information of a user, can alter them and by holding the resources for infinite time it can also collapse the whole system. There are different types of malware attacks, like SMS attacks, Bluetooth attacks, Premium rate attacks,

phone jail breaking etc. Grayware does not cause any damage to a system, but for the commercial purpose it uses some applications or access data from the device. Spyware is the most dangerous in this category, as it pretends to be something different where the actual function of it, is to monitor the activity of the victim and send than activity report to the attacker.

Rooting one's smart mobile phone may present higher dangers of fruitful malware attack. Some altered platform are less all around kept up than pre-installed ones. They likewise frequently give offices to any installed apps to effortlessly pick up root benefits. Subsequently, rooting a smartphone may represent a high security hazard [5].

E. Security Management

There are several security managements are available in the market, like- anti-virus, firewall, Access control, Spam filter etc. etc., but majorly they can be clubbed together into three major category.

Table 4: Types of Security Management.

Types	Description
System Modification	Changes the system's core level coding of kernel. But very much expensive to do.
System add-on	Modifies the configuration files and make them more stick to the rules. It is easy to do compared to before but all the apps need to re-install to handle compatibility error.
Add-on Applications	Easy install as an application. Easy to adopt but totally depends on user.

To guarantee confidentiality and integrity in smartphone, application developers and smartphone client can embrace cryptographic technology. Cryptography can be actualized two ways, application and APIs.

The next table (Table 5) describes the types of different security managements and the threats those can be reduce for that.

Table 5: Security Management.

Type	Mechanisms	Description	Related threats
System Modificati	Firewall	Blocks un-allowed connections, prevents network attacks by denying untrusted networks	T3, T8
	Access Control	Gives limited access to system resources. This	T1, T7

		limits the risk of malwares	
	Authentication	Prevents from unauthorized access of device.	T7
	Pre-Testing	This ensures only the verified developers and ensures the security of an application	T1,T4, T5
	Regular Update	Updating your OS and application regularly can prevent a lot of attacks	T5
	Remote Access Control	When user lose his/her phone, remote access control can stop exposing his/her private information from that device.	T7
System Add-on	Secure API	Secure API ensures the cryptographic security on an application data exchange	T1, T2, T8
Application & Add-on	Anti-Virus	Scans files, folders, SMS, MMS, emails, URLs to prevent malware and phishing attack.	T1, T6, T8
	Spam Filter	Helps to block MMS, SMS, and emails from unknown commercial sources.	T1

F. Conclusion

These days, cell telephones are confined to voice administrations as well as utilized for searching web, playing recreations, sending interactive media messages, versatile managing an account. Numerous industry expert are utilizing their complex cell phones which enhances their profitability yet classified information of their venture moves outside of the protected border of the endeavor. Accordingly new security dangers are developing.In present, there are numerous explores on cell phone security, however there is absence ofpush to examine all security dangers of cell phone. To set up cell phone security, security dangers taking into account cell phone environment is important. Along these lines, in this work, we examined security of cell phone and depicted pertinent security systems against dangers.

G. References:

1. AtulKahate*"Cryptography and Network Security"*, published by McGraw Hill Education (India) Private Limited, pp-8-11.

2. G.P. Picco, *"Lime: Linda Meets Mobility*", ICSE98 International Workshop on Computing and Communication in the Presence of Mobility, April 25, 1998".

3. Mulliner, C.R.: Security of Smart Phone, Master's Thesis of University of California (June 2006)

4. www.ringtoindia.com

5. W. Jeon, J. Kim, Y. Lee and D. Won, "A Practical Analysis of Smartphone Security". Springer-Verlag Berlin Heidelberg 2011, pp. 311-320

6. Good Technology Mobility Index Report Highlights Enterprise Mobility Shift from Devices to Applications, Aug 12, 2014 | Sunnyvale, CA.

7. Rahul B. Mannade, Amol B. Bhande "*Challenges of Mobile Computing: An Overview*", International Journal of Advanced Research in Computer and Communication Engineering.

8. Soeung-Kon, "*Mobile Cloud Computing Security Considerations"* ,Journal of Security Engineering, Jan 2012.

9. SrikanthPullela, *"Security Issues in Mobile Computing" ,* Department of Computer Science University of Texas at Arlington.

10. Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra, "A Survey on Security for Mobile Devices", Vol 15, Issue 1. IEEE 2012.

11. PradipLoganathan "The Challenges and Requirements of Mobile Computing".

12. Dharma P. Agrawal , Hongmei Deng , RajaniPoosarla and SugataSanyal, "*Secure Mobile Computing"*, Distributed Computing - IWDC 2003,Volume 2918 of the series Lecture Notes in Computer Science pp 265-278. Springer Publication.

13. Ashish Wadhaval ,Rugved Mehta and AshleshaGawade, "*Mobile Commerce and Related Mobile Security Issues"*, International Journal of Engineering Trends and Technology (IJETT) – Volume 4, Issue4- April 2013. pp-668-670.

14. "*A Brief Guide to Android Security"* /Ryan Farmer www.acumin.co.uk/download_files/.../ android_white_paper_2.pdf

15. P. Mahesh, A. Jayawant and G. Kale, "*Smartphone Security: Review of Attacks, Detection and Prevention*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, Issue 3, March 2015, pp-141-145.

16. "*Review of Malware Defense in Mobile Network using Dynamic Analysis of Android Application",* Miss. Ashwini A. Dongre, Dept. Of Computer Science and engineering P.R.Patil College of engineeringAmravati, Prof.C.J.ShelkeDept.of Computer Science and engineering, P.R.PatilCollege of engineering Amravati,India

17. https://report.kaspersky.com/

18. https://securelist.com/analysis/quarterly-malware-reports/36303/information-security-threats-in-the-first-quarter-of-2010/

19. LoviDua and Divya Bansal, "*Review on Mobile Threats and Detection Techniques*", International Journal of Distributed and Parallel systems Vol.5, No.4, July 2014.

Corresponding Author:

Kaushik Roy*,

Email: *kroy.compsc@gmail.com*