International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.04, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Mobile Device Security

[1]Abhishek Raghav, [2]Ms. Anuradha Singh, [3]Ms. Preet Thareja

[1]Student M.tech SE, [2,3]Asst. Professor CSE, WCTM

ABSTRACT

Portable devices are today used in all areas of life thanks to their ease of use as well as their applications with unique features. The increase in the number of users, however, also leads to an increase in security threats. This study examines the threats to mobile operating systems. Addressing the four mobile operating systems (Android, Apple OS (iOS), Symbian and Java ME) with the highest number of users, the study provides statistical information about the features of the corresponding operating systems and their areas of use. In the study, the most important threats faced by the mobile operating systems (Malware, Vulnerabilities, Attacks) and the risks posed by these threats were analyzed in chronological order and the future-oriented security perspective was suggested.

I INTRODUCTION

The internet, used by ourselves in all areas of our daily lives, has shown a great improvement in recent years. Accordingly, the devices to connect this virtual environment have undergone a great change and the use of mobile devices has quite increased. Almost all communication and processes can be carried out through the mobile tools (documents, social network, online shopping *etc*.) facilitating the daily life. The increase in this number, however, brings along some security problems.

The unknown Wi-Fi settings, accepting all unidentified applications, connecting to untrusted sites and downloading applications from such sites can be listed as the major ones of these problems. It is of great importance that certain safety precautions should be taken for the mobile tools in which private information and documents of the users are stored. This study examines the operating systems of the most-preferred mobile tools and the threats towards these operating systems and provides detailed information about them.

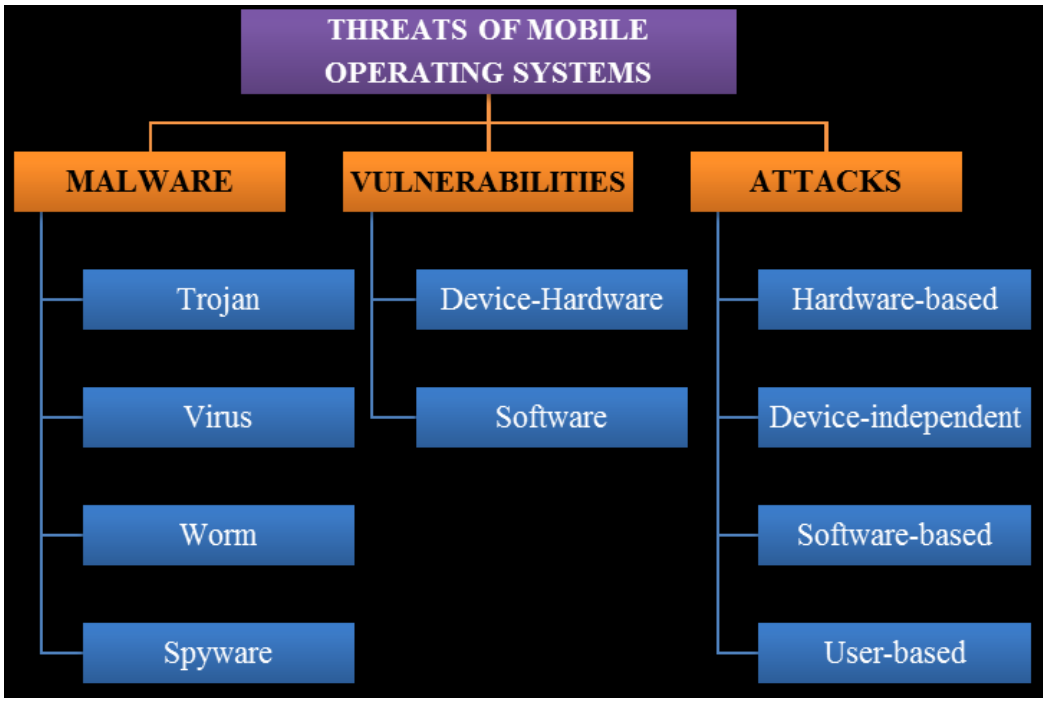
Mobile device usage — smartphones and tablets — is rapidly growing throughout the world. Mobile devices are expected to outsell traditional personal computers. As these devices become ubiquitous, their inherent risks become more apparent.

Security features common on desktop and laptop computers are inconsistently applied across mobile device platforms. On a laptop, we rely on anti-virus software to safeguard our system, but few mobile devices have such

software. While most personal computers on campus are password-protected, few of us configure our mobile phones with a password or PIN to protect it against unauthorized use. And the potential for unauthorized use increases because mobile devices are easily (and frequently) misplaced. While most of us pay attention to system updates and security patches for our computers, mobile device owners focus more on the latest app or features.

II THREATS OF MOBILES DEVICES AND THEIR OPERATING SYSTEM

As all devices with a internet connection, there are also a wide variety of threats to the smart devices using mobile operating system. In line with the portable devices, the malicious software industry is also growing both in technological and structural terms. These threats are discussed in three main categories including Malware, Vulnerabilities and Attacks[1]



2.1 Malware

Malicious Software (Malware) are, in its simplest expression, the malicious software aimed at private specific information which disturb users, may cause breakdown of the device and lead to results such as causing information and documents belonging to the user to be stolen or become unusable . These illegal software which are not installed by the user are used for all attacks from the outside taking advantage of the vulnerabilities in the device or system. The major ones of these software are Trojans, Worms, Virus and Spyware. The first known malware is Cabir which was created for the Symbian operating system in 2004. Cabir is a malicious software which infected the Nokia 60 series and affected many smart phones. This worm writes the word "Cabire" on the screen of the phone infected and

uses Bluetooth connection to spread itself. Apple is more protected against OS malware software thanks to its closed system. The OS which becomes the target of Malware attacks most is Android OS. The biggest reason for this is that the applications can be obtained from many secure-insecure sources.[2]

- Trojans: The main purpose of Trojan software is not to spread themselves but to seize the device management and information. With this aspect, they differ from the worms and viruses. The most widely used spyware are, in this respect, the keyloggers. The purpose of these software transmitted under the cover of another file and unintendedly activated by the user is to get the device entirely under control in the background. These malware are generally carried inside a more innocent software and not noticed by the user. For this reason, while downloading an application necessary for the smart devices, it is of utmost importance to use checked and reliable software. However, this is a little harder for the Android devices. Because, those who use such devices are also able to download applications from elsewhere other than the Google App Store. And even, since they can recognize the external units such as USB or SDcard, the Trojans can also get into the devices through such devices and create a vulnerability in the system. This is a bit more difficult for iOS compared to the Android devices. Because Apple Store constitutes the only option to download application.

- Virus: These are the malicious software which have some features such as penetrating into the existing documents and sending them elsewhere, distorting their contents and making them unusable and slowing down the hardware elements. For the spread of viruses, infected programs should also be installed in other devices. In other words, the infected program must also be sent to other devices by the user. For example; in 2010, the "Zombie" virus infected more than 1 million smartphones in China and caused a loss amounting to $300,000 per day. Besides its numerous damages, it also leads to data loss, data leakage and even disruption of the conversation.

- Spyware: Spyware software are used to collect information on a specific subject. Though specifying that they are used for advertising and promotional purposes (adware) or to provide better service to users (cookies), these software collect information about a person or organization and send those information to someone else without their consent. In this sense, it works like a Trojan and can be used by malicious people. It is also a software aimed at taking control of the devices infected.

2.2 Vulnerabilities

The weaknesses occurring in the system security procedures, internal controls, design and applications are among the security vulnerabilities in the device. These vulnerabilities can be grouped under several headings. In the present study, the analyze is carried out in two main categories including device-hardware vulnerabilities and mobile operating system and application (software) vulnerabilities[3]

2.3 Device-Hardware Vulnerabilities

The most-encountered problem which should be considered first in this regard is the agedness of the device. Because, the manufacturers do not support the devices manufactured before a certain date. Therefore, the device may not receive security updates.

The second issue, however, is the inability of the mobile devices in assuring the safety of the ports they use while connecting to a network or the Internet. The fact that the mobile devices have generally no "navigation" limit used in the Internet environment and there is no firewall to control this is an important vulnerability. A hacker can easily access to the mobile devices via this unsecure port. In such cases, the software called "firewall" which protect these ports must be used. Thus, the user will be asked for permission while connecting to the mobile device and will be able to see it. There may be unauthorized changes ("jailbreaking" or " rooting") on the mobile devices which are not using a firewall. Jailbreaking which provides an escape for Apple iOS is the method applied to obtain an application that does not belong to Apple (iTunes, App store.) or cannot be downloaded due to some restrictions from any other source. This method allows having access to the operating system of the mobile device and this constitutes a vulnerability. In addition, the "jailbroken" devices may not receive security updates of the manufacturer and the devices without the necessary updates may become vulnerable to threats.

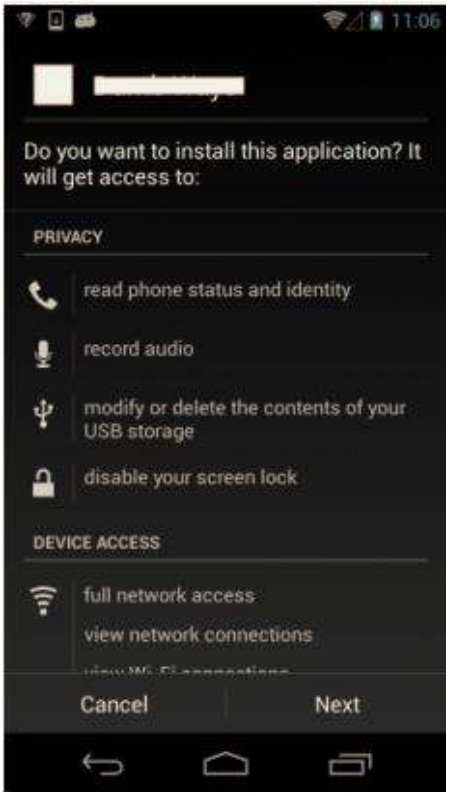
2.4 Software Vulnerabilities

The out-datedness of the mobile operating system is also an important vulnerability. Yet, the best known of the security vulnerabilities arising from software is the use of an old Mobile OS and out-datedness. For example, an Android supports application installation from Google Play or another file system. Since Google file system is a protected area, the downloads or packages (APKs) from this area are secure. However, downloading APK files from third-party application stores, mobile ad libraries and local storage units (*i.e.*, sdcard) is often unprotected. Such vulnerabilities are tried to be met by the firms through new versions or patches.

The shared open source common components also constitute an important vulnerability. Another vulnerability occurring in all open source software is in the design of the system containing common open source components such as WebKit and Linux kernel. These components have a reusable structure in order to reduce the costs and this is a common practice in large open source systems such as Android. A vulnerability has been discovered in WebKit or Linux, however, a patch was released in order to use in solving this problem. Apple's iPhone-like WebKit and BSD kernel derivative (Darwin) constitutes the common software components. The problem at this point is not its re-use but where it is employed. In this regard, Android has put the patch model into practice with a little delay.

The vulnerabilities occurring during the installation of APK files are very common. The presence of a vulnerability known as "Check Time" of the package installer has also been identified. This means that it is replaced by an open APK file or can be changed during installation without the user's knowledge. This open package constitutes the vulnerability of the installer and affects APK files downloaded from unprotected local storage units

As shown in Figures 7, the vulnerabilities largely arise from the permissions given during the installation of an application. Figure 7-(a) shows the permissions required during the installation of an application downloaded from the Google Play to the Android operating system. All these permissions leave the device wide open to the malware. Users should bear in mind that all permission given can be used by the malware. Figure 7-(b) shows the permission display of an APK application. The system first start the installation process of the APK file through the Package Installer and gets critical information such as application name, application icon, application requests and security permissions. When the user intends to install the application, he/she verifies his/her authorization through these permissions and this is called "Time to Check". In all Android applications; the user selects "Next" to continue with the user setup process following this step.



When the user gives such permissions, a vulnerability occurs in the background and the allowed package is replaced by a malware package. Following this process, once the user clicks the "Install" button (—Time of Use"), the Package Installer which will install the APK file installs a different application instead of the set allowed.

In the report released by Symantec; while the number of vulnerabilities affecting the mobile operating system was 315 in 2011, this number increased to 416 in 2012. However, this number declined to 132 with a decrease of 68 % in 2013. It is seen that the number of vulnerabilities in the mobile tools has significantly decreased in 2013. The major reason for this decline is that the companies (especially Android-Google) developing mobile OSs have eliminated

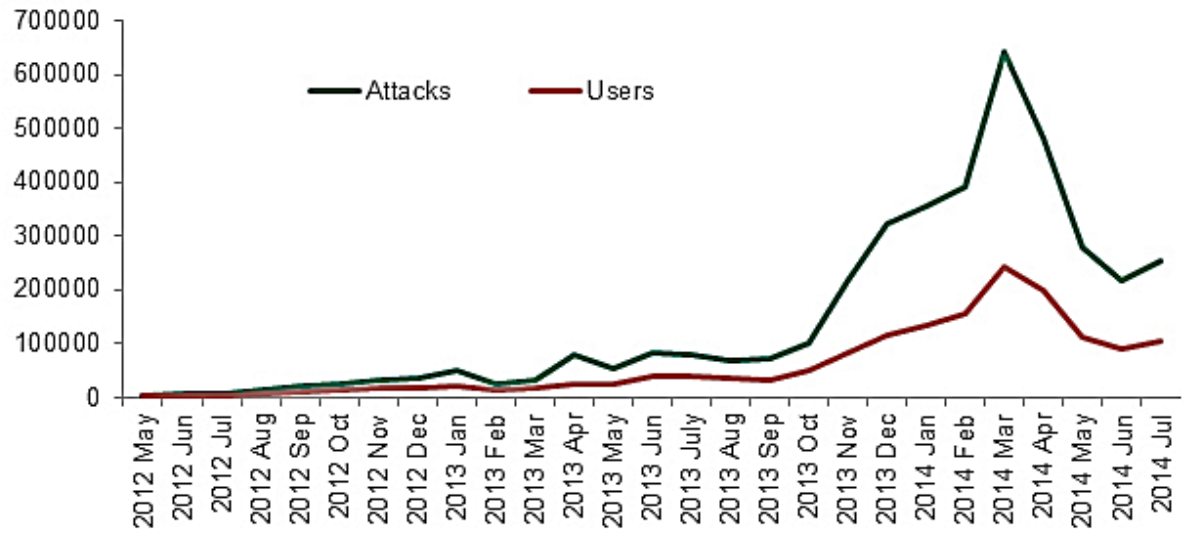
such vulnerabilities through the patches developed by themselves. At the same time, releasing updates at regular intervals for the mobile OSs is the most important factor in maintaining security even against the newly-released malware.[3]

2.5 Attacks

Attacks are the interferences made from outside using a variety of vulnerabilities. This interference are all considered as an attack regardless of whether they are made through malware software or they use vulnerabilities in the smart device or mobile operating system. However, the terms "attack" is generally defines as the attacks made by the hackers for obtaining users' private information without their knowledge.

The first real attack against smartphones was first made by two researchers called Vincenzo Iozzo and Ralf Philipp Weinmann in March of 2010 in order to steal a database from a phone via SMS. This attack was made by looking at an error in the Safari Browser of iPhone 3GS phones and it was aimed to upload the file sent by SMS to the server.

In November 2010, however, an attack was directed to the browser in the Android operating system using a common vulnerability. More recently, the first ―over-the-air‖ attack for GSM software which will lead to memory corruption has been introduced again by Weinmann . Moreover, Oberheide and Lanier has identified several different attack vectors for the iTunes App Store .



The Relationship Between The Number Of Mobile Device Users And The Number Of The Attacks Between The 2nd Quarter Of 2012 And 3rd Quarter of 2014[4]

Above figure shows the relationship between the number of mobile device users and the number of the attacks between the 2nd quarter of 2012 and 3rd quarter of 2014. Accordingly, it is seen that the number of attacks hits the top in March and April of 2014, however, and then starts to decline.[4]

There are various classifications in terms of attacks. One of them is the classification made by Becher which groups the attacks towards mobile devices in four main categories. Hardware-based, device-independent, software-based, and user-based attacks .

-Hardware-based attacks: With a broad perspective, hardware-based attacks constitute an element of mobile security. Even if the Mobile Device has any vulnerability, it cannot easily reach to the user information, however, there is an access to the device.

-Device-independent attacks: These are the attacks independent from the device which directly target the mobile device user. They intend to violate the privacy of the user's personal data through wireless connection or wiretapping.

-Software-based attacks: An important part of the technical vulnerabilities on mobile devices are the software-based attacks. Especially the increase in the number of mobile web browser has led to an increase in the vulnerabilities used in this field.

-User-based attacks: Such attacks are not technical attacks. These constitute the attacks made through cheating without using malicious software which are direct to the mobile device users. These attacks made through "social engineering" and aimed at reaching to private information are today quite common. A large number of the attacks are not technical-based. For example; the Denial of Service (DoS) attacks are not directed through applications or malware installed in smartphones but using the vulnerabilities created by the malformed text messages.[5]

In addition to these attack vectors, there are also other types of attacks. However, the aim of all attacks are essentially to find the victim's vulnerabilities and to make attack using a well-intended process and application.

-JTAG (Joint Test Action Group) Attacks: JTAG is the best-known hardware and debug standard. Even though it provides a high control and observability, it also creates vulnerabilities because of allowing for the control of the device at a deep level.[6]

-Forensic Analysis: This is an attack vector targeting the privacy of the data stored on the mobile devices. This vector applies to the cases where the attacker has physical access to the device. The attacker takes the device of the user who do not realize this situation under his/her control for a certain time. In such a case, the attacker can reach to the information stored in the device. The second possibility is, however, to obtain the confidential corporate data and personal conversations and today, some studies show that this is the most commonly used method.[7,8]

-Phishing Attacks: This is a kind of attack formed by combining the words "Password" and "Fishing". Phishing in the mobile applications is a threat related to the successful attacks reported. This is an OS-independent method and can be used for all types of devices. Such attacks are made through directing the user to the imitation websites instead of the legitimate ones in order to steal their private information such as credentials, credit card information,

user name or password. There are some varieties of this attack such as Similarity attack, Forwarding attack, Background attack and Notification attack. [9]

-QR Code Based Attacks: This is an application which has become very popular recently thanks to its large storage capacity due to the QR (Quick Response) code, ease of production and distribution and the fast readability features. However, users usually are not able to understand the type of knowledge contained in it while scanning QR codes content of which are easily encoded. And this provides a suitable environment to direct users to malicious URLs. Google Safe Browsing API and Phishtank API increases the speed in detecting phishing and malware attacks as well as malicious URLs (SafeQR).[10]

-SSL Proxy Attacks: Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption used in many applications today (especially in internet banking) is a protocol that generally reassures users and provides data security. SSL is an encryption scheme and provides adequate security when implemented correctly. Otherwise, applications may be encountered with security threats and unintended vulnerabilities occurs. If this code is left unreviewed, the settings can be changed in an undesired manner and the information which were presumed to be safe and transmitted can be stolen through communication path.[11]

III PROTECTION AGAINST MOBILE VIRUSES

At the moment there are several anti-virus solutions designed to protect mobile devices from viruses: Kaspersky Lab's Anti-Virus for Windows CE (Pocket PC, Windows Mobile) Symbian (versions 6, 7 and 8 and UIQ) and also for Palm OS (no viruses have yet been discovered for this operating system). Other vendors such as Trend Micro, Network Associates and F-Secure produce similar programs, as do some of the younger companies which specialize in producing dedicated antivirus solutions for mobile devices (Airscanner, Simworks).

As for worms which propagate via MMS, the optimal solution is for the mobile network operator to install an antivirus product on the internet server through which MMS traffic passes. This will ensure protection for the network's users.

IV SOLUTIONS TO ENHANCE MOBILE SECURITY

For organizations, they can increase mobile security by unifying the architecture of the network system. They can unify wireless network, wired network and (VPNs) into one centralized. Highly secured, encrypted infrastructure. That will help monitor the network more closely, who in and who out. It will also help them detect threat faster than if it was decentralized. They can perform performance test using ethical hackers7 . In addition, Transport layer could be encrypted with a PKI(Public Key infrastructure) to ensure the proper authentication and authorization is performed. Workshop, and training programs are necessarily for employees to help increase such security. For individual use, a user can obtain a higher security by following the next tips: Users should use password protection

to unlock the device, change password frequently, and should avoid using common used passwords. Moreover, users should install anti malware, Anti spam and on device personal firewall to minimize the device vulnerability. Moreover, installing such software will help fight against SMS/MMS communications attacks. Phones should have locked back up ,and should be backed and restores remotely and regularly .Also, There should be monitoring tools that a user could take advantage off, to monitor the device activity for any leakage & inappropriate use of information. The device speed, it's functionality, and the speed of network connections could be signs of malware if it happened suddenly.

All in all, mobile devices provided convenience, and increased productivity in today's industries. They are a big exposure to information that could not be easily exposed otherwise. With care and captiousness, all above threats could be prevented, managed, or at least minimized. With the increase advantages of using third party application, user's review is always a good way to check the application authenticity.[12]

V TRENDS AND FORECASTS

It is difficult to forecast the evolution of mobile viruses with any accuracy. This area is constantly in a state of instability. The number of factors which could potentially provoke serious information security threats is increasing more quickly than the environment – both technological and social – is adapting and evolving to meet these potential threats.

The following factors will lead to an increase in the number of malicious programs and to an increase in threats for smartphones overall:

- The percentage of smartphones in use is growing. The more popular the technology, the more profitable an attack will be.
- Given the above, the number of people who will have a vested interested in conducting an attack, and the ability to do so, will also increase.
- Smartphones are becoming more and more powerful and multifunctional, and beginning to squeeze PDAs out of the market. This will offer both viruses and virus writers more functionalities to exploit.
- An increase in device functionality naturally leads to an increase in the amount of information which is potentially interesting to a remote malicious user that isstored on the device. In contrast to standard mobile phones, which usually have little more than an address book stored on them, a smartphone memory can contain any files which would normally be stored on a computer hard disk. Programs which give access to password protected online services such as ICQ can also be used on smartphones, which places confidential data at risk.

However, these negative factors are currently balanced out by factors which hinder the appearance of the threats mentioned above: the percentage of smartphones remains low, and no single operating system is currently showing dominance on the mobile device market. This currently acts as a brake on any potential global epidemic – in order to

infect the majority of smartphones (and thus cause an epidemic) a virus would have to be multiplatform. Even then the majority of mobile network users would be secure as they would be using devices with standard (not smartphone) functionality.

Mobile devices will be under serious threat when the negative factors start to outweigh the positive. And this seems to be inevitable. According to data from the analytical group SmartMarketing, the market share of Symbian on the Russian PDA and smartphone market has been steadily increasing over the last 2 to 3 years. By the middle of 2005 it had a market share equal to that of Windows Mobile, giving rise to the possibility that the former may be squeezed out of the market.

Currently, there is no threat of a global epidemic caused by mobile malware. However, the threat may become real a couple of years down the line – this is approximately how long it will take for the number of smartphones, experienced virus writers and platform standardization to reach critical mass. Nevertheless, this does not reduce the potential threat – it's clear that the majority of virus writers are highly focussed on the mobile arena. This means that viruses for mobile devices will invariably continue to evolve, incorporating/ inventing new technologies and malicious payloads which will gradually become more and more widespread. The number of Trojans for Symbian which exploit the system's weak points will also continue to grow, although the majority of them are likely to be primitive (similar in functionality to Fontal and Appdisabler).

The overall movement of virus writers into the mobile arena is an equal stream of viruses analogous to those which are already known with the very rare inclusion of technological novelties and this trend seems likely to continue for the next 6 months at minimum. An additional stimulus for viruses writers will be the possibility of financial gain, and this will come when smartphones are widely used to conduct financial operations and for interaction with epayment systems.

VI. CONCLUSION

Our main aim is to secure mobile devices and apps and protect the people that use them. Now a days mobile app testing, device monitoring, forensics and security intelligence capabilities provide us with a unique set of mobile security data.

We also aim to help and secure the mobile devices and apps that connect with their corporate assets each day. IT and security teams should take care of the following key points:

- Mobile security requires a different approach not focused on malware. Leaky apps that store or transmit sensitive personal and corporate data in an insecure manner are of far greater concern at this point in time.

- Even legitimate apps without intentionally malicious functionality that are downloaded from official app marketplaces can include high risk security issues.
- Mobile security requires identifying and remediating security issues in device OSs and configurations, the apps installed on those devices, and the network connections those devices make each day.

VII. FUTURE DEVELOPMENT

The largest problem with mobile security is there is no enough time dedicated to it when designing a mobile device. For the most part, the malware can only access if the user does something to make the system vulnerable in some way or fashion. Be it running a program that has the malware hidden in it, or cracking the system so that the built in security is removed. Many experts argue that the only thing that will make users more aware is a large amount of malware forcing people to become educated or else leave them unable to use their devices. The reason for this is because in the early 2000 there were a large number of viruses that completely debilitated networks. This in turn made people understand the importance of antivirus and their threats that they don't recognize. Since then, people have been much more careful with their computers. Due to this positive response, many people think this is the only way to make people pay attention to mobile devices security. In example, there have been many proofs of concept viruses that target phones just to show it can be done and explain it could have been even worse; however this generally is circulated through the technical world and never reaches the end users on a large scale.

REFERENCES

[1] A. Axelle, ―The Evolution of Mobile Malware‖ , Computer Fraud & Security vol. 2014, no. 8, pp. 18–20

[2] L. Qing and C. Greg, ―Mobile Security: A Look Ahead‖ , IEEE Computer and Reliability Societies, (2013), pp. 78-81.

[3] C. Gao, and J. Liu, ―Modeling and restraining mobile virus propagation‖ , IEEE Transactions on Mobile Computing, vol.12, no.3, (2013), pp. 529-541.

[4] http://2010.hack.lu/archive/2010/Weinmann-All-Your-Baseband-Are-Belong-To-Us-slides.pdf

[5] A. Greenberg, Google pulls app that revealed Android flaw, issues fix, 2010, http://news.cnet.com/8301-270803-20022545-245.html.

[6] [Mobile Cyber Threats, http://securelist.com/analysis/publications/66978/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/, , Last accessed 25 March 2015.

[7] M. Becher, ―Security of smartphones at the dawn of their ubiquitousness‖ , Ph.D. dissertation, University of Mannheim, (2009).

[8] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck and C. Wolf, ―Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices‖ . In Security and Privacy (SP), (2011), pp. 96-111.

[9] K. Rosenfeld and K. Ramesh, ―Attacks and Defenses for JTAG‖ , IEEE Design & Test of Computers, vol.27, no. 1, (2010), pp. 36-47.

[10] C. Boyd and P. Forster, Time and date issues in forensic computing—a case study. Digital Investigation, vol.1, no.1, (2004), pp. 18-23.

[11] [34] F. C. Freiling, T. Holz and M. Mink, ―Reconstructing People's Lives: A Case Study in Teaching Forensic Computing‖ , In IMF, (2008). pp. 125-142.

[12]Ongtang, Machigar, Stephen Mclaughlin, William Enck, and Patrick Mcdaniel. "Semantically Rich Application-centric Security in Android." Security and Communication Networks: N/a. Print.