Research Journal of Applied Sciences, Engineering and Technology 8(24): 2381-2387, 2014
DOI:10.19026/rjaset.8.1244
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: June 08, 2014 Accepted: July 19, 2014 Published: December 25, 2014

Research Article

Demanding Requirement of Security for Wireless Mobile Devices: A Survey

K. Muthumanickam and E. Ilavarasan
Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry-605014, India

Abstract: Today, the technology advancement in telecommunication facilitates users to bear portable devices with convenient and timely accessing to their personal and business data on the fly. In this regard, mobile and ubiquitous devices become part of the user's personal or business growing. Recently, the usage of portable devices has drastically amplified due to wireless data technologies such as GPRS, GSM, Bluetooth, WI-Fi and WiMAX. As the use of wireless portable devices increases, the risks associated with them also increases. Specifically Android Smart-phone which can access the Internet may now signify an ultimate option for malware authors. As the core open communication mediocre, the Airwave, is susceptible, there has been a rise of a security technique suggested by researchers. When comparing to security measures proposed to protect wireless devices, protecting mobile vulnerabilities is still immature. So in this study, we present an organized and widespread overview of the research on the security elucidation for wireless portable devices. This survey study discusses the security risks imposed by vulnerabilities, threats and security measures in the recent past, mainly spotlighting on complex attacks to user applications. We classify existing countermeasures at guarding wireless mobile devices facing different kinds of attacks into various groups; depend on the revealing technique, collected information and operating systems. In the next phase we will design and implement new security model to protect mobile phone resources against unknown vulnerabilities.

Keywords: IDS, mobile threats, security, WiFi-AP

INTRODUCTION

Many people around the world make use of the Internet everyday. Providing uninterrupted connectivity has turn out to be essential for people's business or personal life nurturing reliance on electronic communication over the Internet. Mobile wireless devices such as cell phones, PDAs and smart phones (here forth, referred Mobile phones) are now indispensable individual and business communication tool which represents today's fastest growing technology. Even traditional computers are not advancing as fast as this technology. The total number of mobile subscription users was 96.2% in 2013 which was 15.5% in 2001 (ITU Statistics, 2014). Every day the number of mobile phone users is growing hurriedly. Unfortunately, the popularity of mobile phone makes them an ideal target for malware writer also. At the start, mobile phones have run standard Operating System (OS) which suffered from heterogeneity issue. This weakness permits malware writers to exploit a single vulnerability to assault a huge number of devices which is a key for security eruption (Kotadia, 2007). Recently, the development of OS for mobile device has increased as shown in Table 1, each mobile phone OS has a considerable market share.

We can anticipate various different mobile phone malware threats with advanced techniques in the future. Furthermore, as users increasing exploit mobile phones to the Internet banking or online shopping, malware writers make use of this opportunity to insert malicious software into a mobile phone and compromise its safety measures. Then, attackers can able to propagate the same malware on the Internet. As evidence that malware attackers are targeting mobile environment, there has been a tremendous increase in the number of reported mobile vulnerabilities (Corporation, 2014).

In order to understand the current security issues which threatens mobile phones, this study describes threats, sophisticated mobile vulnerabilities and software attacks and also scrutinize a number of security measures to protect mobile platforms.

LITERATURE REVIEW

This section explains different glossary notations exercised in wireless telecommunication and

Corresponding Author: K. Muthumanickam, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry-605014, India

Table 1: World wide mobile phone sales in end users of operating system in 3Q13 (Gartner Research, 2013) (thousands of units)

Company	3Q13 units	3Q13 market share (%)	3Q12 units	3Q12 market share (%)
Android	205,022.7	81.9	124,552.3	72.6
IOS	30,330.0	12.1	24,620.3	14.3
Microsoft	8,912.3	3.6	3,993.6	2.3
Blackberry	4,400.0	1.8	8,946.8	5.2
Bada	633.3	0.3	4,454.7	2.6
Symbian	457.5	0.2	4,401.3	2.6
Others	475.2	0.2	683.7	0.4
Total	250,231.7	100	171,652.7	100

networking technologies. Additionally, we enlighten Android, a popular OS for mobile phones.

Wireless telecommunication technologies: It has been widely identified that information is power. Today, we can access information from anywhere, anytime, even on the fly. Like the traditional Personal Computer (PC)s, the progression of wireless technologies has also been characterized as different generation.

First generation: This generation uses the analog technology for information communication. It makes use of Frequency Division Multiple Access (FDMA) to support multiple users access the communication medium. For example, Advanced Mobile Phone Service (AMPS) in US.

Second generation: The Second generation utilizes the combination of Time Division Multiple Access (TDMA) and FDMA. For example, Global System for Mobile Communications is the first wireless communication technology was built in 1990 by a study group named Group Special Mobile formed in 1982 by the Conference of European Posts and Telegraphs (CEPT). The main intention of GSM is to provide uninterrupted service to users. Additionally, it supports voice over circuits, digital fax, web access, call forwarding and Short Message Service (SMS).

Two and half generation: The next phase was the 2.5G technology, which shows better performance with a higher data transfer rate over GSM and TDMA-based wireless cellular infrastructures. The General Packet Radio Service (GPRS) another technology that makes use of packet switching mechanism to transfer data between subscribers. Additionally, GPRS supports multimedia applications and third party services to attract mobile users. In order to support higher reliability and bandwidth, Enhanced Data rates for GSM Evolution (EDGE) standard was introduced in 2000.

Third generation: 3G uses spread spectrum method for medium access. Universal Mobile Telecommunication System (UMTS) is an example of 3G network. 3G offers higher transmission rate when compare to its predecessor 2G and 2.5G networks. Moreover, in 3G, both data service and voice service use packets.

Wireless networking technologies: As wireless technology provides flexibility and convenience, wireless communication has been applied mainly in the field of Wireless Local Area Network (WLAN). This wireless technology allows users to access data and network system even they move into the premises of broadcasting area. There are few classes of WLAN standards that control communication such as IEEE 802.11, HyperLAN, HomeRef, Bluetooth and MANET. The two most popular WLANs in the mobile environment are defined as follows.

IEEE 802.11: This standard supports two different types of operation modes. First, infrastructure based network in which a device called an Access Point (AP) acts as a central controller to regulate medium access, coordinate and connect communicating devices in a WLAN. Secondly, infrastructure-less based networks in which there is no central controller to coordinate any activity. So each mobile device includes all necessary functionalities. The popular protocols defined in IEEE 802.11 are given in Table 2.

Bluetooth: This technology is maintained and managed by the Bluetooth Special Interest Group which permits users to compose an ad hoc wireless connection to transfer data within short distance (50 m) with data transfer rate of 720 kbps. As Bluetooth utilizes unlicensed 2.4 GHz ISM frequency band, it is integrated into almost all mobile devices. There are three different classes in Bluetooth technology as given in Table 3.

Android OS: Android is an open source platform for mobile wireless devices built up by Google. The

Table 2: IEEE 802.11 popular protocols

Standard	Bandwidth (GHz)	Ritrate (Mbps)
802.11a	5 UNII	Upto 54
802.11b	2.4 ISM	Upto 11
802.11g	2.4 ISM	Upto 54

Table 3: Three classes of bluetooth technology

Type	Power	Distance coverage (m)
Class 1	20 dBm	100
Class 2	4 dBm	10
Class 3	0	1

Linux-based Android OS offers subsystems such as Window management and applications with different aspect of functionality. For Android OS, applications are implemented as a Java program using JAVA Native Interface (JNI). However, it uses Dalvik byte code which is similar to a virtual machine devised to execute applications with low-memory. The android device also allows digitally signed third party applications to install.

METHODOLOGY

Mobile phone malware: This section describes a wide-ranging summary of mobile phone malware and security measures offered to mobile wireless portable devices.

What is a mobile malware? A mobile malware is malicious software which is designed to infect mobile wireless devices without the customer's knowledge. It can be distributed using different communication channels. Based on the propagation method and infecting style, malware can be classified as follows.

Virus: A virus is a malicious executable that can insert itself into executable file. Whenever virus files are handled by a user, it can make duplicate copies of itself and inset into another document or executable file.

Worms: Worms are software programs which exist in Random Access memory. They do not need human interaction; instead insert themselves into other files.

Trojans: Trojan Horse is a software program which looks benign application that offers different functionalities to the end-user. However, they hide malicious program.

Rootkit: It is a technique designed to conceal itself from detection applications. It can either whitehat or blackhat. The latter type can be used to compromise and uphold remote control over the victim computer for a prolonged period of time. Rootkits are platform-independent.

Botnet: Robot Network is a collection of compromised computers, which can later be used to perform many computer illegal activities. This network is controlled and maintained by its owner called, Botherder. Botnet together with rootkit technique becomes really a most serious threat to the Internet users.

First mobile malware appeared early in 2004 targets the Symbian OS (Trend Micro, 2012). Mobile malware can be dispensed through different ways, such as accessing the Internet via a mobile browser, downloading applications from stores, installing executable using Bluetooth and MMS. This kind of malicious software can be used for corrupting user data, make mobile device inoperative, sending a premium SMS without user's consent, providing backdoor, corrupting user applications and blocking external memory cards. Compare to the wired communication medium, propagating a virus through wireless backbone produces more benefits to malware authors:

- If an operation on the victim AP does not look anomalous, detecting malicious attacks can be possible using only WiFi frames.
- Existing forensic tools and methods are not sufficient to identify the volume and existence of malware infected equipment such as the number of communication to victim IPs.
- Detecting a virus which propagates using WiFi-AP pose additional challenges.

Related works: Ortega Juan *et al*. (2011) proposed a method for locating Trojan horse mobile malware in Bluetooth enabled mobile devices. Their idea was based on monitoring all incoming connection requests during send or receives files through Bluetooth devices. Kaskersky Lab (2010) discusses a Trojan horse that targets Android mobile phones. This malware gets downloaded when a user visits porn videos and expect user interaction for installation. After installed, the malware begins transmitting money from the user's account to its owner's account. Bickford *et al*. (2010) Presented how malicious rootkit techniques affect mobile devices. After a mobile malware has been installed, which includes rootkit technique, the malware owner can access sensitive information. Different malicious rootkit samples, perform different activities. For example, a rootkit sample permits a remote attacker to listen keenly to confidential GSM exchange, can try to violate the user's privacy by sending a text message from the compromised mobile phone to its owner's location or can exploit power exhaustive in GPS or Bluetooth enabled mobile phones to drain the battery. Recently, researchers (Milliken *et al*., 2013) have discovered a new type of mobile virus Chameleon that escalation through the air like an epidemic disease. The chameleon can infect both WiFi-Access Point (AP) and PCs. It compromises an AP by patching the existing firmware to obtain credentials. Then, it can steal data about all users' who are associated with that AP. As Chameleon spreads through air, traditional antivirus tools cannot easily detect them. Another noted point about this malware is, it can disseminate more quickly where WiFi APs are densely appearing. The propagation principle of the Chameleon mobile virus, is given as follows:

i. Identifies and locate all venerable APs within a specific network or region

Table 4: History of mobile malware

Year	Malware type	Target OS	Infection method(s)
2005	Worm	Symbian	Doom 2 video game
	Trojan	Windows	File infection
	Virus		Fake SIS application
	Cross-platform		Auto starting external memory
			Replacing font files
			Infecting the OS
2006	Worm	J2ME	Dropping method
	Trojan	Symbian	Infection through CIL
	Spyware		Infection via e-mail
	Cross-platform		Overwriting system files
			Fake browser or commercial software
2007	Worm	Symbian	Spreading via bluetooth
	Trojan		Pretend to be ICQ application
			Proof of concept
2008	Worm	Windows mobile	Spreading through fake applications using MMS and bluetooth
	Trojan		Spreading via memory card
2009	Worm	Symbian	Spreading via malicious URl
	Botnet	iPhone	Fake application
	Spyware		
	SMS exploit		
2010	Worm	Cross-platform	Fake SMS
2011	Trojan	Android	Infection into legitimate applications using third party files
	Multifarious Malware	iPhone	Scanning IPs and connecting to SSH
2012	Trojan	Android	Installing additional malicious applications
	Malware	Windows mobile	Obfuscating class names
2013	Botnet	Android	Through C&C
	Malware		Replacing firmware in WiFi-AP
	Ransomware		Fake antivirus

ii. Evade the security solutions and admin interface available on the AP
iii. Identifies and stock up the AP system settings
iv. Inject virus firmware on the victim AP by replacing the legitimate AP firmware
v. Reload the victim AP system settings
vi. Propagate viruses; go to (i)

Table 4 shows a report of notable mobile malware from 2005 to 2013.

Growth of mobile malware: Due to the growth of mobile malware, many papers have given a statistical report on them. Hypponen (2006) discussed an overview and statistics of mobile malware from 2004 to 2006. F-secure security solution has listed 401 different classes of mobile malware in 2008; however McAfee has found 457 classes of mobile malware (Lawton, 2008). During 2004-2010, F-Secure have cataloged 517 classes of mobile worms, virus and Trojan horse (Hyppoene, 2010). Juniper Networks (2011) Mobile threats report stated a 400% raise in Android OS since 2010. According to International Data Corporation (IDC) Android OS and Windows Mobile would raise about 50% during 2010-2014 which becomes the leading mobile phone OS hawkers in the future (Corporation, 2014). At the same time, the growth of mobile malware may also increase exponentially. AV-TEST found that millions of Android mobile phones are presently connecting the Internet with no antivirus applications. In Toyssy and Helenius (2006), the authors discussed and classified mobile malware that targets mobile phones based on the platform and infection mechanisms.

The mobile device platforms: Symbian, Windows CE and Windows Mobile, RIM Blackberry, iPhone OS, Palm OS and Linux.

The infection mechanisms: Bluetooth, MMS, IP connection through GPRS, EDGE, UMTS and external memory card.

Many authors suggested some security countermeasures to protect mobile devices against malware attacks:

- The users should use the mobile device in a protected way by installing and running antivirus software.
- The security software vendor can develop and supply necessary security applications.
- The network operator can have IDS tools to detect and prevent intrusions.
- The device manufacturer can supply and update software patches automatically which restricts the attackers success rate.

In December 2011, the AV-TEST GmbH laboratory (AV-TEST Gmbh Lab. http://www.av-test.org/en/) has recorded a total over 8000 mobile malware. Within next one month, in January 2012, the count has increased to a huge total of over 21,000 that targets Android OS. This expansion clearly indicates that cyber criminals believe

the mobile platform to be a latest source of income. Most recently, the attractive way for propagating malware is by integrating infecting applications with fake antivirus applications. As, Google play application store on the Internet has consistently verified apps, malware criminals avoid them and instead proffer apps directly from the website. The idea is to transport malicious files and data from PCs to mobile phones. Mobile phone users can avoid malware attacks by installing a certified antivirus application. But failures can allow the malware to run riot.

Forecasting and prospective threats: Since the introduction of first mobile phone, predictions and discussions about mobile threats aiming these devices have proliferated. The first mobile malware threatens Palm OS and Symbian OS (Leavitt, 2000) in 2000 but never turn into widespread and there were no massive attack threats until 2010. Panda Security Lab (http://press.pandasecurity.com/wp-content/uploads/) reported that more than 56% malware created in 2011, whereas in 2012, it increased to 76.57%. However, worms and virus development dropped to 11.33 and 9.67% respectively. But in 2013, there was 30 million new malware created at an average of 82,000/day. Sophos Security Lab has recorded over 300 malware families in their database (http://www.sophos.com/en-us/medialibrary/PDFs/other/). Recently, malware writers developed Android botnets for controlling and stealing information from Android mobile phones. For example andr/GGSmart-A, botnet uses Command & Control (C&C) mechanism to communicate all Android devices it has compromised. Unlike earlier Android attacks, botnet can change and control premium SMS numbers and content. In 2013, Sophos discovered android Defender, a ransomware attack which demands the user to pay $99.99 to resolve the problem.

Juniper MTC (http://www.juniper.net/us/en/local/pdf/additonal-resources) pointed out that tablet deliverance will outpass the overall PC market by 2015. And also, it points out that all mobile platforms grew 614% from 2012 to 2013 with a 155% increase accounted in 2011. Prior to 2011, a vast amount of mobile malware was released targeting Java ME device 70.3% and Nokia Symbian 27.4%. However, in 2011, 46.7% of malware were created aiming Android OS. Kotadia (2007) reported that 2013 was the year of mobile malware attacks diversification towards Android OS with 98.5%.

Mobile security: Malware is a software program designed to violate the security features, gather sensitive information, or gain access to the victim computer or mobile device. Compared to malware attacks against traditional computers, mobile wireless malware attacks are very costly and become a serious threat in the future. For example, the network operator is responsible of blaming cost even if an event caused by a malware in the mobile device without user's permission. Additionally, there are many factors limit the use of sophisticated security solutions for preventing malware attacks in a mobile device.

A complete IDS algorithm that can function effectively on a PC cannot be effortlessly transported to mobile phone. We also ensure that the security measures do not drain the CPU time to evade battery exhaustion (Becher *et al*., 2011). In Oberheide *et al*. (2008), the clamAV malware detector engine accessible for Nokia mobile phone needs around 1 min to initialize the signature database with 40 MB of memory. In order to decrease this operating cost the authors perform each mobile antivirus operation in offline.

When compared to traditional PCs, the security measures of mobile phones are relatively different and complex. A single sophisticated mobile device presents many wireless technologies which permit users to connect the Internet from anywhere at any time. The author of Mulliner (2006) listed different metrics which distinguish traditional computer security from wireless mobile device security, such as device mobility which is small in size so that it can be easily tampered or stolen, user's personalization, wireless connectivity that allow users to do transaction through the Internet, technology confluence to allow a mobile device to host multiple technologies and limited capabilities. In Oberheide and Jahanian (2010), the authors pointed out that mobile phones have limited computational ability and power utilization which is not sufficient to run a behavioral detection algorithm for discovering advanced mobile threats. Additionally, the use of communication medium, Air, makes the wireless information exchange more vulnerable. The utilization of a microphone which acts as a sensor can also be targeted for sniffing user's personal data. The mobile device may comprise of many files which need to be restricted in right to use especially while accessing third party applications.

SECURITY MEASURES FOR MOBILE PLATFORM

In this section we analyze different mobile malware detection mechanisms to avert the different threat that target mobile platforms. Table 5 summarizes the detection rate of different mobile security protection applications (http://www.av-test.org/fileadmin/ pdf/avtest_2013-01_android_testreport_english.pdf).

Intrusion detection for mobile phone: Intrusion Detection System (IDS) on mobile phones can be either prevention-based or detection-based method. The former method uses hash functions, unique digital signatures, cryptographic algorithm to provide confidentiality, integrity and authentication service. The latter approach can be based on anomaly-based or signature-based or hybrid-based approach.

Table 5: A top 10 manufacturer's product that offers mobile security application for Android in 2013

Rating	Vendor	Product	Detection rate (%)
1	Antiy	AVL	100
1	Bitdefender	Mobile security	100
1	TrustGo	Mobile security	100
2	Lookout	Antivirus and security	99
3	Avast	Mobile security	98
3	Symantec	Mobile security	98
4	Comodo	Mobile security	97
4	Dr. Web	Antivirus	97
4	NQ mobile	Mobile security	97
4	Tencent	QQ security	97
4	TrendMicro	Mobile security	97
5	Kaspersky	Mobile security	96
5	Sophos	Mobile security	96
5	Webroot	Secure anywhere mobile	96
6	ESET	Mobile security	95
7	AhnLab	V3 mobile	94
7	F-secure	Mobile security	94
8	Quick heal	Total security	93
9	G data	Mobile security	89
10	IKarus	Mobile security	87

The paper (Ho and Heng, 2009) proposed a Java-based platform independent engine to control the functions and spreading nature of mobile malware. This generic model blocks the automatic transmission of malware executable files from a conciliated mobile phone through e-mail, instant messaging, MMS, infrared and Bluetooth. In Damopoulos *et al*. (2012), four different machine learning algorithms have been utilized to spot illegitimate utilization of the iPhone. Their detection is based on behavior classification through telephone calls and SMS using a SHA-1 algorithm. This approach produces a higher detection rate with higher true positive rate. Shabtai *et al*. (2011) presented a host-based general IDS framework for discovering malware in Android mobile phones based on supervised anomaly detection approach. This method uses metrics such as number of active processes, number of outgoing packets and CPU consumption. Their simulation results prove that Naïve Bayes and logistic regression classifiers outperforms than other classifiers. The IDS proposed in Jacoby *et al*. (2006) was based on monitoring power consumption. They collected data by measuring energy consumption over a period of time for generating power signatures. Finally, the generated signatures are used to detect known attacks. Portokalidis *et al*. (2009) conferred a method to identify malware attacks by hosting Anti-malware detection software on the secure server instead of keeping and running them on the mobile phone. Their framework on the device side interrupts each system call and signal which later rechecked to look for inconsistency on the server. Though this approach protects a mobile device, the reprocessing operations on the server would increase the response time.

The authors of Zhu *et al*. (2009) implemented a graph based method for controlling MMS/SMS-based mobile worms. The Mobile phones which have close communication have partitioned using network vestige which can later be used for constructing a social relationship graph. In this way, an optimal cluster of patched mobile phones can be identified and isolated from the cell. Becher and Freiling (2008) developed a framework that runs on a mobile phone as a background process. Their framework called, MobileSandbox, monitor and analyze each system Application Programming Interface (API) call invoked during an application executes. Zahid *et al*. (2009) collects keystroke data from 25 mobile phones and then 6 unique keystroke features have extracted for precisely recognize mobile user. The simulation results confirm an error rate of 2%. SMS-Watchdog in Yan *et al*. (2009) monitors and collects SMS message transaction over a period of 5 months and dynamically analyzes them to detect anomalies using four different detection approaches that built legitimate social activities profile for each user which then used for detecting anomalous SMS user. As each user can occupy only a countable memory state SMS-Watchdog compel minimal overhead. The anomaly based detection approach shows a detection rate of 92% with 8.5% of false alarm rate. However, AMA-Watchdog detects 66% of SMS-based attacks with no false alarm.

CONCLUSION

Today, Wireless, mobile world and applications are turning out to be greatest growing IT field. It brings several changes and improvement in business and human's personal lives. As both mobile devices and applications are used for merrymaking online banking to critical censorious business applications, malware creators continue to get better profitability using quicker go-to-market strategies. Though many security solutions and techniques exist for detecting and preventing a PC from malware attacks, they cannot be suitable for a mobile environment due to limited resource availability.

In this study, first of all we have discussed the evolution of mobile malware threats, by epitomizing its progression with examples. We have also delineated

reports on forecasting the near future mobile threats and the seriousness of Chameleon, a WiFi-AP virus that spreads through the air. Also, we have been suggesting some existing security solutions based upon IDS. This study deals with a wide-ranging overview of mobile malware threats from surveying from scratch to current need. This study may be useful for researchers to receive relevant research problem. In near future, we will plan to design and implement a policy based authentication mechanism to shield mobile phone resources against unknown vulnerabilities.

REFERENCES

Becher, M. and F.C. Freiling, 2008. Towards dynamic malware analysis to increase mobile device security. Sicherheit, 128: 423-433.

Becher, M., F.C. Freiling, J. Hoffmann, T. Holz, S. Vellenbeck and C. Wolf, 2011. Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. Proceeding of the 2011 IEEE Symposium on Security and Privacy (SP), pp: 96-111.

Bickford, J., P. O'Hare, A. Bliga, V. Gnapathy and L. Iftode, 2010. Rootkits on smart phones: Attacks, implications and opportunities. Proceeding of the 11th Workshop on Mobile Computing Systems and Applications, pp: 49-54.

Corporation, S., 2014. Symantec internet security threat report 2014. Vol. 19, 2014.

Damopoulos, D., S.A. Menesidou, G. Kambourakis, M. Papadaki, N. Clarke and S. Gritzalis, 2012. Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers. Lect. Notes Comput. Sc., 5(1): 3-14.

Gartner Research, 2013. Gartner Says Smart Phone Sales Accounted for 55 Percent of Overall Mobile Phones in Third Quarter of 2013. Retrieved from: http://www.gartner.com/newsroom/id/2623415/.

Ho, Y.L. and S.H. Heng, 2009. Mobile and ubiquitous malware. Proceeding of the 7th International Conference on Advances in Mobile Computing and Multimedia (MOMM '09). ACM, USA, pp: 559-563.

Hyppoene, M., 2010. Mobile security review september 2010. Helsinki Finland Technical Report, F-Secure Labs, September 2010.

Hypponen, M., 2006. Malware goes mobile. Sci. Am., 295(5): 46-53.

ITU Statistics, 2014. Retrieved from: http://www.itu.int/ict/statistics.

Jacoby, G.A., R. Machany and N.J.D. Iv, 2006. How mobile host batteries can improve network security. IEEE Secur. Priv., 4: 40-49.

Juniper Networks, 2011. Malicious mobile threats report 2010/2011. Technical Report, Juniper Networks Inc.

Kaskersky Lab, 2010. Popular Porn Sites Distribute a New Trojan Targeting Android Smart Phones. Retrieved from: http://www.kaspersky.com/news?Id=207576175.

Kotadia, M., 2007. Major Smartphone Worm by 2007: Gartner Study. June 2005. Retrieved from: Media.kaspersky.com/pdf/KSB-2013-EN.pdf.

Lawton, G., 2008. Is it finally time to worry about mobile malware? Computer, 41: 12-14.

Leavitt, N., 2000. Malicious code moves to mobile devices. Computer, 33: 16-19.

Milliken, J., S. Valerio and M. Alan, 2013. Detection and analysis of the chameleon WiFi access point virus. Eurasip J. Inform. Secur., 2013: 1-14.

Mulliner, C.R., 2006. Security of smart phones. M.A. Thesis, University of California.

Oberheide, J. and F. Jahanian, 2010. When mobile is harder than fixed (and vice versa): Demystifying security challenges in mobile environments. Proceeding of the 11th Workshop on Mobile Computing Systems. ACM, USA, pp: 43-48.

Oberheide, J., K. Veeraraghavan, E. Cooke, J. Flinn and F. Jahanian, 2008. Virtualized in-cloud security services for mobile devices. Proceeding of the 1st Workshop on Virtualization in Mobile Computing. ACM, USA, pp: 31-35.

Ortega Juan, A., F. David, A.A. Juan, G.A. Luis and V. Francisco, 2011. A novel approach to Trojan horse detection in mobile phones messaging and bluetooth services. KSII T. Internet Inform. Syst., 5(8): 1457.

Portokalidis, G., P. Homburg, N. FitzRoy-Dale, K. Anagnostakis and H. Bos, 2009. Protecting smart phones by means of execution replication. Tech. Report, Vrijie Universite, Amsterdam.

Shabtai, A., U. Kanonov, Y. Elovici, C. Glezer and Y. Weiss, 2011. Andromaly: A behavioral malware detection framework for android devices. J. Intell. Inform. Syst., 38: 161-190.

Toyssy, S. and H. Helenius, 2006. About malicious software in smart phones. J. Comput. Virol., 12(2): 109-119.

Trend Micro, 2012. Retrieved from: http:// countermeasures. trendmicro.eu/ wp-content/ uploads/2012/02/History-of-Mobile-Malware.pdf.

Yan, G., S. Eidenbenz and E. Galli, 2009. SMS-watchdog: Protecting social behaviors of SMS users for anomaly detection. Proceeding of the 12th Symposium on Recent Advances in Intrusion Detection, pp: 202-223.

Zahid, S., M. Shahzad, S. Khayam and M. Farooq, 2009. Keystroke-based user identification on smart phones. Lect. Notes Cpmput. Sc., 5758: 224-243.

Zhu, Z., G. Cao, S. Zhu, S. Ranjan and A. Nucci, 2009. A social network based patching scheme for worm containment in cellular networks. Proceeding of the IFOCOM 2009, pp: 1476-1484.