A Review of Malicious Code Detection Techniques for Mobile Devices

Lamia Ketari and Mohammadi Akheela Khanum

***Abstract*—With the advent and rising popularity of wireless systems, there is a proliferation of small-enabled devices such as PDAs, mobile phones, etc. While these devices are becoming more and more preferable by all age groups, they also pose the threat of being vulnerable to malicious code (e.g.: viruses, trojans, worms, etc). In fact, the mobile devices rely on open and public transmission media. Besides, open platforms are becoming popular in smart phones. In this context, these devices have become more capable, providing users with all conveniences, ranging from traditional phone usage to supporting multiple features like e-mail access, playing games, software downloading and also e-banking. As the capabilities of these devices increase, the threat of malicious code (also called malware) targeting them also increased. It is believed that the evolution of mobile malware will take a similar direction as the PC malware. In this paper, we conducted a questionnaire based survey to know about the mobile device security concern among the users. The results indicate a high awareness but a low use of strong security measures. Then, we explore the various mobile phone vulnerabilities. A review of malicious code detection techniques for mobile devices are presented and discussed.**

***Index Terms*—Malware, malicious code detection techniques, mobile devices.**

I. Introduction

In recent years, mobile phones have evolved from supporting telephonic functions to supporting multiple features, ranging from capturing and playing digital media, to e-mail access, e-banking [1], and remote access to personal files. As the capability of mobile phones is increasing, the threat of malicious code targeting them also is increasing. It is widely believed that the evolution of malware for mobile devices will take a similar direction as the evolution of PC malware. Many operations involving sensitive data transfer, such as financial transactions, online buying and selling of goods, are being done excessively through the mobile devices. Mobile devices are easy targets for malware because they are well connected, incorporating various means of wireless communications [18]. Similar to PCs, the mobile devices are capable of Internet access for web browsing and emails. They also have the capability to communicate by wireless LAN, short range Bluetooth connectivity, and short/multimedia messaging service (SMS/MMS). Also one of the most important reasons cited in the literature for mobile devices to be the target of malware, is the population of users. According to 3Gtech[1] report of January 2010, everyday, there are more than one million new additions to the GSM family of technology users receiving service from one of the 700 commercial GSM networks across 218 countries and territories around the world. Chris Pearson, President of 3G Americas, stated that this level of wireless technologies growth exceeds that of almost all other lifestyle-changing innovations. Because mobile devices have become similar to PCs, many operations involving sensitive data transfer such as financial transactions, online selling and buying of goods are being done excessively through mobile devices. The malware targeting mobile phones developed slowly in the past six years since the first proof-of-concept mobile malware called Cabir[2] was discovered in 2004. According to Gartner,Inc.[3] report of May 2009, worldwide mobile phone sales totaled 269.1 million units in the first quarter of 2009, while worldwide PC shipments only reach 292 million units in the whole year of 2008. These figures are alarming, as a large scale outbreak of mobile malware could be more serious than the PC malware. In the Section II, we examine the types of attacks also present some reasons which motivated us for undertaking this work. Section III.

II. Background and Motivation

Malware outbreaks in wireless networks constitute an emerging research topic [2]. In November 2006, Web poll of corporate IT administrators by security vendor Sophos reported that 81% of respondents express concern over malware and spyware targeting mobile devices will become a significant threat. However, 64% said they have nothing in place to secure their smart phones and PDAs [3]. As the number of mobile devices in the world has expanded dramatically in recent years, the amount of malware targeting the mobile devices also increased [3]. We briefly examined the work by Dagon et.al [4], to understand the types of attacks against mobile devices on the basis of securities attackers hope to achieve. Table I depicts the classification established by the authors.

TABLE I: Mobile Attack Taxonomy

Security Goals	Types of Attacks
Confidentiality	Theft of data, bluebugging and bluesnarfing
Integrity	Phone hijacking
Availability	Denial-of-service attacks and battery draining

Manuscript received February 20, 2012; revised March 31, 2012.

Authors are with the department of Information Technology in College of Computers and Information Sciences, at King Saud University, Kingdom of Saudi Arabia (e-mail:lketari@ksu.edu.sa, kakheela@ksu.edu.sa).

1 3Gtech, http://www.3gtech.info/25-billion-gsm-subscribers-worldwide.html

2 Viruslist, http:// www.viruslist.com/en/analysis?pubid=200119916

3 Gartner, Inc., http://www.gartner.com/it/page.jsp?id=985912

Theft of data: Hackers often attack mobile devices to obtain transient information and static information. Transient information includes the phone's location, its power usage, and other data, which the device does not normally record [4].They attack on static information that cellular devices store or send over the network. These attacks try to get data such as contact information, phone numbers, and programs stored on smart phones. The bluesnarfing and bluebugging attack are examples of data theft. The bluebugging attack allows unauthorized access to the phone and may include listening to calls made from and to a victim's phone. Initially, bluebugging was limited to merely listening in and as an extension, recording these conversations. However, this attack has progressed to being able to manipulate the various functions of the phone [4]. For example, an attacker can use a victim's phone to make calls, send messages and carry out any task that the phone can do. On the other hand, the bluesnarfing attack consists in an unauthorized access or retrieval of data from applications like calendar, inbox, contact list, and gallery via Bluetooth [4]. Downloading information is done using various tools, specifically designed for bluesnarfing.

Phone Hijacking: Some malware might attempt to use the victim's phone resources. Possibilities include placing long-distance or 900-number calls, sending expensive SMS messages, etc. The recent Mosquitos virus is one example [4]. Pirated copies of a computer game were infected with a virus that sent expensive SMS messages when users played the illicit copy of the game. Hijacking phone resources is not unexpected – malware authors have been using victims' resources for quite a while.

Denial-of-Service (DoS): According to Dagon et al. [4], DoS could be done by flooding the device and draining power. At present, it is extremely easy to crash or overwhelm most Bluetooth applications on mobile devices just by sending repeated pieces of information, corrupted packets, and incorrect file formats. However, power demands always constrain mobile devices, so this latter category is believed to be more serious. DoS is still the dominant attack type that can be exploited from the known vulnerabilities [2].

Looking to the attack history, many Trojans, Worms, Viruses have entered the mobile world and have affected them. According to F-secure, there were more than 350 mobile malware in circulation by the end of 2007 [9]. Examples of some well known threats on Symbian-based smart phones include Skull, Cabir and Mabir [4]. Many variants of these viruses have reinforced their attacks, revealing an unprecedented and an alarming level of exposure. However, many of them lack a good understanding of risks and controls related to various security technologies [5]. According to McAfee's[4] 2008, mobile security report, nearly 14% of global mobile users had been directly infected or had known someone who was infected by a mobile virus. The number of infected mobile devices has a strong increase in McAfee's[5] 2009 report.

We conducted an exploratory survey to examine users' awareness of mobile device security issues. The main motivating factor for the review of malicious code detection techniques is the result of this survey that we carried out on a population of 41 mobile device users mostly females in the age group of 18-34 years, who are studying IT at graduation level. We received 41 responses. The key findings of the survey are:

- Most respondents (78%) use a smart phone as their mobile device, with blackberry taking over iPhone.
- About 81% respondents are aware of the antivirus.
- 30% respondents always connect their mobile device to Internet.
- 83% respondents download software from the Internet to their mobile devices.
- Very few of the respondents use antivirus as a defense mechanism against their mobile device infection by malicious code.
- Nearly half of the respondents were not concerned with the security of their mobile device.
- 43% respondents cited Internet usage as their favorite functionality through mobile device.

The graphical representation of the survey results are depicted in Fig.1 through Fig.5.

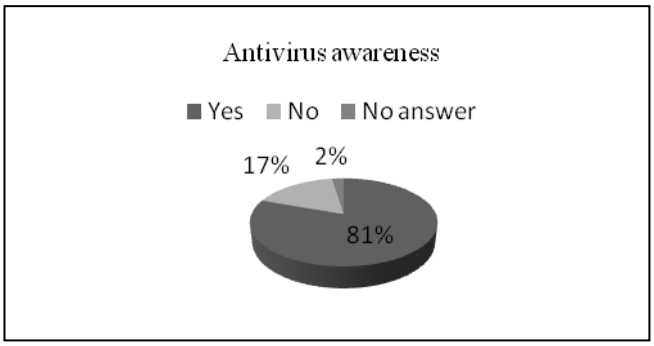

Fig. 1. Antivirus Awareness

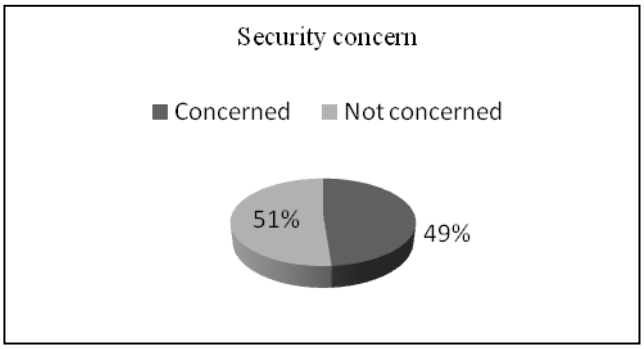

Fig. 2: Security concern

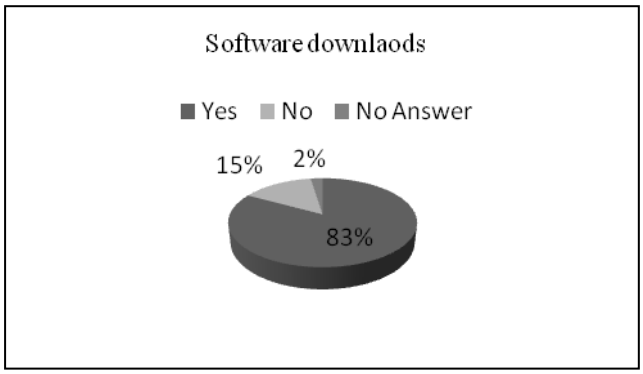

Fig. 3: Software downloads

4 http://www.mcafee.com/us/research/mobile_security_report_2008.html

5 http://www.mcafee.com/us/local_content/reports/mobile_security_report_2009.pdf

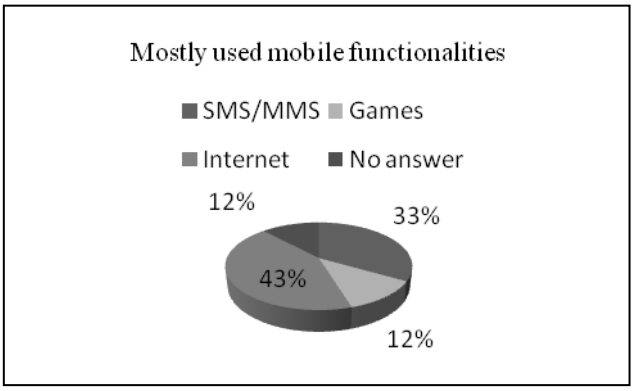

Fig. 4: Mostly used functionalities

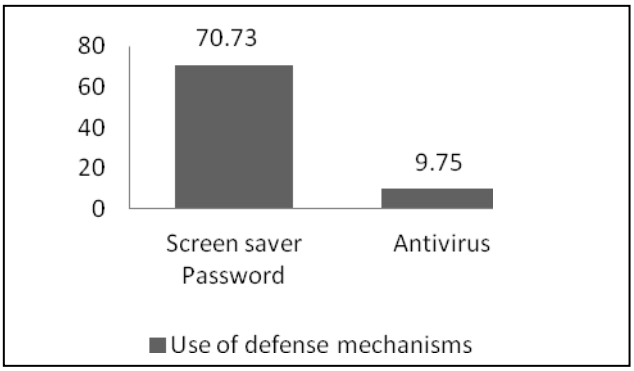

Fig. 5: Use of defense mechanism

III. Literature Review

Lately, a surge of interest has been expressed in malicious code detection techniques in mobile devices. Mainly, three approaches were explored:

- **Signature-based detection** is a popular technique based on searching for previously defined virus signatures in input files [6]. Signature detection has the advantage of detecting malicious activity before the system is infected by the malicious code.
- **Behavior checking** is another popular technique based on a behavior checker that resides in the memory looking for unusual behavior. In this case, the user is alerted. Behavior checker has a disadvantage that by the time a malicious activity is detected, some changes have already been done to the system.
- **Integrity Checker** is a technique that maintains a log of all the files that are present in the system. The log may contain characteristics of files like the file size, date/time stamp and a checksum. Every time an integrity checker is run, it will check the files on the system and compares with the characteristics it had saved earlier.

In what follows, we present some relevant related work that refers to the above mentioned malicious code detection techniques.

In [6], the author has described a signature representation method for detecting viruses in mobile devices. He used hash table to store virus signature hash values for fast matching. To speed up the matching process, he used first matching signature cuts which represent portion of signatures least likely to occur in normal files before matching the entire signature. This method was tested on Symbian OS Nokia 6682 device. The results indicated that scanning using a hash table is 98% faster than sequential scanning. The drawback of this system is that it cannot detect new malware that is very different from previous ones. Therefore, it needs to be combined with more advanced malware detection methods, such as heuristic scanning and detection based on network activities. As viruses have evolved, the technologies for defending them also had to evolve. In this context, malicious code detection involves more advanced approaches, such as heuristics and behavior analyzers, that is collectively refer to as “non signature” detection methods [14].

In [7], the authors describe an intelligent heuristic method to detect viruses in the mobile devices. The method uses Dynamic Link Libraries (DLLs). The list of DLL functions used by virus indicates the behavior of the virus in terms of its functionality. This approach is able to detect new viruses that have the similar functionalities as existing ones. The method was tested on Symbian-OS platform and obtained 95% detection on all the viruses and 0 false positive on non-virus programs.

In [8], the authors have presented a behavior checking system. The system is a collaborative virus detection and alert system for smart phone called SmartSiren. The system has a light-weight agent running on each smart phone. A centralized proxy is used to assist the virus detection and alert processes. The agent keeps track of communication activities on the device and periodically reports a summary of these activities to the proxy. The proxy performs joint analysis on the received reports and detects any single-device or system wide viral behaviors. When a potential virus is detected, the proxy sends alerts to both infected devices and a subset of the uninfected devices, which may be in direct contact with an infected device. The use of proxy reduces the processing burden from the resource constraint smart phones and it also simplifies the collaboration among the smart phones. The results indicated that SmartSiren prevents wide-area virus outbreaks with affordable overhead.

In [9], the authors describe a machine learning algorithm to detect malicious activities in mobile devices like the smart phones. The anomaly detection is done by a remote anomaly detection system. Each smart phone acts as a client, sending a set of features which are extracted by learning the various measurements of the resources, hardware and software components to the remote anomaly detection system, where these features are stored into a database. The database is accessed by detection units which analyzes the data for malicious activity. The method was tested on Symbian-OS and Windows Mobile and results indicate that the methods saves considerable amount of the disk space also the computation and communication costs were also reduced which has a positive impact on the battery lifetime.

In [10], the authors have described behavior-based malware detection in mobile phones called pBMDS. pBMDS uses a probabilistic approach through correlating user inputs with system calls to detect suspicious activities in mobile phones. It observes unique behaviors of mobile phone applications and the operating users on input and output constrained devices. In addition, it leverages a Hidden Markov Model to learn applications and user behaviors from two major aspects: process state transitions and user operational patterns. Built on these, pBMDS identifies

behavioral differences between malware and human users. The results indicated that pBMDS is effective, light-weight and easy to deploy and also has the capability to detect unknown malware.

In [11], the authors describes a framework for a background monitoring system which collects the software that a user is going to install on its device and to automatically perform a dynamic analysis of the software. The analysis system uses the mobile network as analysis place rather than the mobile device for two reasons. First, the mobile network has more computing power to perform a more thorough analysis. Secondly, it is assumed that most software will be delivered via the mobile networks, in part, because of easier handling compared to dealing with local connections. Therefore, before a user installs software on his mobile device, the software will be analyzed in the mobile network for malicious behavior. This is done by automatic dynamic analysis, where system calls are logged and afterwards analyzed for malicious behavior. The dynamic analysis is done in three stages. In the first stage, the software samples are collected. The second stage consists of analyzing the collected samples by a particular module called Mobile sandbox. This module executes the sample in an environment (the sandbox), where it can watch the steps of the investigated sample. This results in sequences of API calls that the program used during its execution. The third stage is responding to the analysis. If a malicious activity is detected then the mobile network operator might choose to disallow the installation of the software. It also might send a message to alert the user that the program violates the user's or network's security profile, depending on how severe the damage is expected to be.

In [12], the authors have described a method called Paranoid Android, for checking the security of smart phones using remote security servers, which has exact replicas of the phones in virtual environment. The servers are not subject to the same constraints as the smart phones, therefore allowing the application of multiple detection techniques simultaneously. Phone's execution is recorded and replayed at the security server in the cloud. When an attack is detected, the Paranoid Android warns the user. If the device is already engulfed by the attack, it can be restored back to, so a previous safe state using the data held at the replica. A prototype of Paranoid Android was tested on Android phones. The results show that transmission overhead can be kept below 2.5KiBps even during periods of high activity and virtually nothing during idle periods, and battery life is reduced by about 30%.

IV. Conclusion

Paper is a survey of malicious code detection techniques for mobile devices. We conducted a questionnaire based survey to know about the mobile device security concern among the users. The results indicate a high awareness but a low use of the strong security measures. The review of various malicious detection techniques indicated that mostly the anomaly detection is done by a proxy away from the source of attack. This type of detection approach has two main advantages: First, the large detection solutions needs huge processing speed and power consumption. Second, the proxy can alert other users of the possible attacks before the whole network is engulfed by malware activities, because reactive approach is always better than proactive. Based upon the rapidly changing attack contour, one cannot be specific about the future of virus detection. But what is required is known, an efficient malicious code detection method which will simply reduce the spread rate and which could be applied at network level in order to protect the routes of spreading. To conclude, it seems likely that the coming malicious code detection techniques will be distributed in nature. It can be believed that the focus will move away from endpoint protection to network wide protection. The study has formed the basis for our future work on malicious code detection dedicated to mobile devices. It has also established the line of investigation that is needed to move forward in developing a framework for network-wide protection.

Acknowledgment

We would like to deeply thank Dr. Areej Al Wabil for her valuable reviewing and suggestions.

References

[1] R. Tiwari, S. Buse, and C. Herstatt, "Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage," *Proc. International Research Conference on Quality,Innovation and Knowledge Management, New Delhi*, Feb.2007, pp.886-894.

[2] Q. Yang, R. H . Deng, Y. Li, and T.Li, "On the Potential of Limitation-oreinted Malware Detection and Prevention Techniques on Mobile Phones," *International Journal of Security and its Applications*, vol. 4, no. 1, Jan. 2010.

[3] G. Lawton, "Is It Finally Time to Worry about Mobile Malware?," *Computer*, vol. 41, no. 5, May 2008, pp. 12-14, doi:10.1109/MC.2008.159.

[4] D. Dagon,T. Martin, and T. Starner, "Mobile Phones as Computing Devices,the Viruses are Coming!," *Pervasive Computing, IEEE*, vol. 3, no. 4, Oct-Dec. 2004, pp. 11-15. doi: 10.1109/MPRV.2004.21.

[5] M. Howell, S. Love, and M. Turner, "User Characteristics and Performance with Automated Mobile Phone Systems," *International Journal of Mobile Communications*, vol. 6, no. 1,2008, pp.1-15.

[6] D. Venugopal, "An Efficient Signature Representation and Matching Method fo Mobile Devices," *Proc. 2nd Annual International workshop on Wireless Internet* (WICON '06), Boston, MA, United States, 2006. doi: 10.1145/1234161.1234177.

[7] D. Venugopal, G. Hu, and N. Roman, " Intelligent Virus Detection on Mobile Devices," *Proc. International Conference on Pirvacy,Security and Trust: Bridge the Gap between PST Technologies and Business Services* (PST'06), Ontario, Canada, 2006, pp.1-4. doi:10.1145/1501434.1501511.

[8] J. Cheng, S. Wong, S. H. Y. Wong, H. Yang, and S. Lu, "SmartSiren: Virus Detection and Alert for Smartphones," *Proc. 5th International Conference on Mobile Systems, Applications and Services* (MobiSys '07), San Juan, Puerto Rico, June 11-13, 2007, pp. 258-271. doi:10.1145/1247660.1247690.

[9] A. Shmidt, F. Peters, F. Lamour, and S. Albayrak, "Monitoring Smartphones for Anomaly Detection," *Proc. 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, 2008.

[10] L. Xie, X. Zhang, J. Seifert, and S. Zhu, " pBMDS: A Behavior-based Malware Detection System for Cellpohone Devices," *Proc. Third ACM Conference on wireless Network Security* (WiSec'10), Hoboken, New Jersy, USA, March 22-24, 2010. doi: 10.1145/1741866.1741874.

[11] M. Becher and F.C. Freiling, " Towards Dynamic Malware Analysis to Increase Mobile Device Security," *Proc. SICHERHEIT* 2008. pp. 423-433.

[12] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, " Paranoid Android: Versatile Protection for Smartphones," *Proc. 26th Annual Computer Security Applications Conference* (ACSAC'10), Austin, Texas, USA, Dec. 6-10, 2010.

[13] H. Kim, J. Smith, and K.G. Shin, "Detecting Energy-Greedy Anomalies and Mobile Malware Variants," *MobiSys '08*, Breckenridge, Colorado, USA, June 17-20, 2008.

[14] A. Shevchenko, "Malicious Code Detection Technologies," *Kaspersky Lab*, Inc.2008. http://latam.kaspersky.com/sites/default/files/knowledge-center/malicious%20code%20detection%20technologies.pdf

Lamia Ketari is Assistant Professor in Information Technology department in the College of Computer and Information Scineces, at King Saud University, Kingdom of Saudi Arabia. She hold PhD in Computer Science from the Concordia State University, Canada. She is actively involved in research in the field of Information Security and Web Services. She has many international conferences and Journals papers to her credit.

Mohammadi Akheela Khanum is Researcher in Information Technology department in the College of Computer and Information Scineces, at King Saud University, Kingdom of Saudi Arabia. She has a vast experience in academics and also in research. Currenlty she is involved with the projects in information security, web services, HCI and usability testing. She has authored many research papers in both international and national conferences and journals.