Research in Progress- Defending Android Smartphones from Malware Attacks

Dr.Marwan Omar
Colorado Technical University
Colorado Springs, USA
marwankhan2003@yahoo.com

Dr.Maurice Dawson
Alabama A&M University
Alabama, USA
dr.mauricedawson@yahoo.com

Abstract— **Smartphones are becoming enriched with confidential information due to their powerful computational capabilities and attractive communications features. The Android smartphone is one of the most widely used platforms by businesses and users alike. This is partially because Android smartphones use the free, open-source Linux as the underlying operating system, which allows development of applications by any software developer. This research study aims to explore security risks associated with the use of Android smartphones and the sensitive information they contain; the researcher devised a survey questionnaire to investigate and further understand security threats targeting Android smartphones. The survey also intended to study the scope of malware attacks targeting Android phones and the effectiveness of existing defense measures. The study surveyed the average Android users as the target population to understand how they perceive security and what security controls they use to protect their smartphones.**
Keywords- Malwar; Android Smartphones; Hacker; Anti-Virus; Cyber Threats; Vulnerability

Introduction

Smartphones are becoming a more integrated and prevalent part of people's daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying. With this fast adoption of smartphones, imminent security threats arise while communicating sensitive personally identifiable information (PII), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks [1], [2]. Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally "proof of concept" attempts to break to the phone's system and cause damage. However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications [3]. Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services [4].

I. THEORETICAL FRAMEWORK

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones' operating systems. [5] indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones, and thus expand the attack surface. For example, in December, 2004, A Trojan horse was disguised in a video game and was intended to be a "proof of concept," which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones [6]. Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users.

With the development of innovative features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more entertainment features than security solutions. In turn, this further increases vulnerabilities and opens doors for hackers to deploy attacks on smartphones. Furthermore, [7] argue that the operating systems of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. This poses more security challenges because hackers could exploit those vulnerabilities, which are further compounded by users' lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop

978-0-7695-4941-5/13 $26.00 © 2013 IEEE
DOI 10.1109/ACCT.2013.69

and laptop computers; smartphones' enhanced features, such as music players and video games, produce easy-to exploit targets by sending seemingly benign files via music or video game applications to users and lure them into downloading such files. [8] indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

II. Research Objectives

The primary goal of this research study is to investigate security risks associated with the use of Android smartphones and then propose to design an effective, real-time, integrated defense framework for Android smartphones. This study will contribute to identifying top security threats facing Android phones and the confidential information they contain. The proposed solution will detect attacks (viruses, worms, and Trojan horses) and prompt users to take actions to prevent breaches; any suspicious activity that may reveal personal information to third parties or unknown entities will be reported to users to prevent potential attacks. Smartphones contain easy-to-exploit vulnerabilities as well as sensitive personal information, which collectively offer appealing motives for attackers to target them to gain financial incentives [9]. A focused review of the literature reveals that there have been many protection strategies offered for securing smartphones and ensuring user privacy; however, most of those endeavors are small-scale and tackle particular areas of protection, such as access control [10] and anomaly detection [11]. This research study is different in that it will leverage previously proposed and implemented defense strategies and present an enhanced protection framework that will address Android's vulnerabilities and risks. Furthermore, this project will extend the existing knowledge about Android smartphones' security and provide in-depth understanding of how to effectively manage emerging threats and fend off attacks, an issue that has long been realized and pointed out by security researchers and required more extensive research [12].

III. The research problem statement

Google's Android is free, open-source software that allows the development and programming of third-party software programs, in addition to being used as a tool to handle e- commerce tasks and perform online banking activities. Android's core components, such as Linux and connectivity media, are vulnerable to attacks through which personal and confidential information is likely to be compromised. Android's threats are further amplified by the fact that users are limited to using their smartphones for basic services and functions, such as email and SMS/MMS. Users lack the programming mind-set to protect their Android smartphones and stay current with the latest security software updates. This gives hackers an edge to target Android smartphones in the hope of gaining unauthorized access to disable core services (email and web browsing), abuse costly services (i.e., sending MMS/SMS and making calls to high-rate numbers), eavesdrop on calls, and most importantly compromise sensitive information to be sold for a price. Android's open-source nature further increases security vulnerabilities because attackers could easily exploit this feature to modify the core applications and install malicious software, which could be used to compromise Android-based smartphones and ultimately cause disruption and monetary loss.

IV. Research Questions

Research Question1: What are the shortcomings of current security practices in Android smartphones?
Research Question 2: Has research fully addressed the importance of protecting sensitive personal data in Android smartphones and recommended defenses and mitigation countermeasures?
Research Question 3: Are the operating systems of Android smartphones able to handle processing power required to implement an integrated security framework to provide real-time security for confidential data?
Research Question 4: What protection mechanisms (i.e., antivirus, access control, intrusion detection, and encryption) have proven to be most robust in protecting confidential data and ensuring user privacy?

Research Question 5: Which attack techniques/vectors (i.e., Bluetooth, Wi-Fi, MMS, video games, music files, and SMS) are most popular among attackers, and what is the extent of their damage?

V. METHODOLOGY

The researcher used a quantitative, descriptive survey design strategy to collect and analyze data from Android smartphone users. Surveys are very commonly used in current research and are considered to best suit quantitative data analysis, in addition to the fact that survey results and findings can be replicated on the same people at different times to further confirm or refute previous findings. A link to the online Android security survey, which was hosted on the popular commercial Survey Monkey website, was sent to 200 Android users, including people from different industries and professions who were randomly chosen as a sample of the population of interest (the population of interest encompassed the average Android users who were of both genders, 18 years old or older, and belonged to a variety of industries and professions). The survey webpage included clear and detailed information about ensuring complete anonymity of research participants as well as maintaining the confidentiality of their identity and the information

provided. Potential respondents were asked to voluntarily take part in the study, and they also had the option of declining to participate or exiting the online survey at any stage during the survey process. The survey was available for five months and ran from August 2012 until December 2012; 45 completed responses were received from the Survey Monkey website.

Also, respondents were required to answer all 25 questions in the questionnaire for their responses to count as complete. The survey questionnaire included 25 questions and was designed to be completed in about 5 minutes to encourage more respondents to take part in the survey and thereby maximize the response rate, which reached about 22%. A response rate of 22% with a sample size of 200 is considered a valid sample size statistically [13]. The researcher ensured that the only data collection method would be to count the responses received from Survey Monkey and that no other responses were counted if they were received in any other form. This data-gathering fashion can guarantee standardization and contribute to the objectivity of research results. A total of 46 people responded to the survey, 45 of whom provided complete answers to all 25 questions. Any incomplete responses were discarded to further validate representativeness of results, as there was only one respondent who did not complete the survey and was listed as an outlier.

The study was conducted anonymously (respondents were unknown to the researcher) to maximize representativeness and minimize potential bias. The researcher did not consider using other forms of data collection, such as sending the survey to potential respondents by first class mail, due to financial concerns and time constraints. Personal interviews were also discarded because respondents are more inclined to express their true experiences anonymously, in addition to the fact that the researcher had decided to conduct this study in a double-blind manner, meaning that potential respondents and the researcher did not know each other. A consent form was attached to the online survey webpage to express anonymity of the research study and ensure respondents' privacy and confidentiality of information collected. The research clearly stated that participation in the survey was voluntary and that all responses would be confidential.

A. About the Pilot Study

The objective of the pilot study was to ensure the appropriateness and adequacy of questions for the sample of interest and incorporate feedback and suggestions from the pilot study participants to enhance the survey and make slight changes on the questions' format and style. For the pilot study, the researcher chose ten respondents who were all Android users and met the criteria for the research population. A link to the online survey was sent via email to ten participants over a period of two weeks. Constructive feedback and valuable insights were received from some participants who suggested a few changes to the way some questions were asked and the choices provided for those answers.

B. Population of Interest and Representativeness of Results

The population of interest was Android users among the general public who were from both genders and over the age of 18; all respondents had at least completed high school and some of them had a college degree. All respondents used Android phones on a daily basis with a vast majority of them downloading apps for a variety of purposes, such as entertainment, financial transactions, and web browsing. A random sample of Android users was chosen from this population where the chances of including any user from any other sample was equal, and therefore, the sample was as representative as possible and the risk of bias was reduced to a minimum. Furthermore, the researcher chose to conduct this study in a double-blind manner where the researcher and respondents did not have any direct communication, nor did they know each other. This method prevented personal prejudices from influencing the results of this study.

C. Data Collection Procedure

A link to the online Android survey hosted by Survey Monkey was distributed to potential respondents, and the researcher created an account with Survey Monkey to save all the responses received. The researcher ensured that the only data collection method would be to count the responses received from Survey Monkey; no other responses were counted if they were received in any other form. This method for gathering data guarantees standardization and contributes to the objectivity of research results. A total of 46 people responded to the survey, 45 of whom provided complete answers to all 25 questions. Any incomplete responses were discarded to further validate representativeness of results, as there was only one respondent who did not complete the survey.

D. Delimitation of The Study

This research study was uniquely designed for smartphones using the Android platform as the underlying

operating system; the research design methodology only encompassed the general public of Android users and advertently excluded participants who would be "tech-savvy" in order to meet the purpose and objectives of the dissertation. Also, the research study did not address any security threats or risks associated with the Android hardware, such as battery life or stealing or losing the phone physically. Furthermore, the results of the study represent what survey participants reported and may not be considered as ideal perspectives. Finally, the findings will not be applicable to other mobile platforms, such as Windows Mobile and Symbian. This study mainly provides insightful solutions for major types of malicious attacks, such as viruses, worms, and Trojan horses; it does not encompass attacks based on exhausting battery power or any other types of attacks outside of the scope of malware attacks.

VI. HYPOTHSES

Hypothesis 1: Current security mechanisms of Android smartphones are ineffective at withstanding well-crafted malware attacks. Authentication measures (i.e., user name and password) and antivirus software are reactive and can only detect known malware. Furthermore, Android, unlike other platforms such as iPhone and Blackberry, does not have any built-in encryption, which in turn makes Android phones attractive and soft targets for malware writers.

Hypothesis 2: The top security risks to Android phones stem from Android apps where hackers can conveniently pass and deliver their malicious apps to the Android Market with no restrictions. The Android Market does not enforce any kind of testing or vetting process to certify apps and filter rogue ones. Moreover, current security mechanisms implemented by the Android platform does not distinguish malicious apps from legitimate ones. Therefore, malicious apps (once installed onto Android phones) can misuse their access to phones' resources and commit unauthorized activity, such as sending users' confidential information to remote servers operated by hackers.

Hypothesis 3: Android devices are exposed to and vulnerable to a variety of threats, which can be exploited by hackers. Examples include threats of rogue and malicious apps, which can abuse their capabilities when accessing the phones' resources and thus send users' private information to remote servers without users' knowledge or consent. Most recently, there was an Android Trojan that was capable of sending SMSs and recording phone calls from victims' smartphones.

Hypothesis 4: Hackers have previously launched attacks on Android smartphones. Therefore, an integrated and effective security solution is required to address vulnerabilities and threats within Android devices.

CONCLUSION

This research will contribute to raising awareness among security experts and the academic community about the impact and consequences of smartphone attacks, which is something that has not yet been fully recognized. This is critically important given the fact that smartphones, if compromised, can be used to cause extensive damage and disruption for individuals and businesses alike. The contribution of this study is further exemplified by extending the body of knowledge for smartphone security and stimulating the need for more extensive research in this area. The contribution will be particularly important because it will present proactive defense strategies and alert the academic community to place more emphasis on making smartphone security a more active area of research. Moreover, those proactive defense techniques will best serve in mitigating risks that are higher than ever before in current mobile environments. This will ultimately contribute to prevention of data loss (which could be sold by hackers for a price), decrease potential lawsuits caused by identity theft, and increase the confidence for smartphone users conducting mobile commerce.

REFERENCES

[1] Wong, L. (2005). *Potential Bluetooth vulnerabilities in smartphones*. Retrieved from http://citeseerx.ist.psu.edu.

[2] Brown, B. (2009). *Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns*. Retrieved from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-security-expert-worries-smart-phone

[3] Bose, A. (2008). *Propagation, detection and containment of mobile malware*. (Doctoral dissertation, University of Michigan). Retrieved from www.phoenix.edu/apololibrary.

[4] Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware*. Retrieved from www.cse.psu.edu

[5] Bhattacharya, D. (2008) *Leardership styles and information security in small businesses: An empirical investigation* (Doctoral dissertation, University of Phoenix). Retrieved from www.phoenix.edu/apololibrary

[6] Rash, W. (2004). *Latest skulls Trojan foretells risky smartphone future*. Retrieved from www.eweek.com.

[7] Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smartphones for security analysis. *Proceedings of the 3rd USENIX Workshop on Offensive Technologies Montreal, Canada*. Retrieved from www.usenix.org

[8] Becher, M., Freiling, F., & Leider, B. (2007, June) On the effort to create smartphone worms in Windows Mobile. *Proceedings of the 2007 IEEE workshop on Information Assurance. United States Military Academy*. West Point, NY. Retrieved from http://pi1.informatik.uni-mannheim.de/filepool/publications/on-the-effort-to-create-smartphone-worms-in-windows-mobile.pdf. .

[9] Portokalidis, G., Homburg, P., Anagnostakis, K., & Bos, H. (2009). *Paranoid Android: Zero-day protection for*

smartphones using the cloud. Retrieved from www.cs.vu.nl/~herbertb/papers/trpa10.pdf.

[10] Ni,X., Yang, Z, Bai, X., Champion, A., & Xuan, D. (2009). *DiffUser: Differentiated user access control on smartphones*. Retrieved from http://www.cse.ohio-state.edu/~champion/pubs/09_wsns_nybcx.pdf

[11] Schmidt, A-D., Peters, F., Lamour, F., Scgeel, C., Camtepe, S., & Albayrak, S. (2009). Monitoring smartphones for anomaly detection. *Mobile Networks and Applications, 14*(1), 92-106.

[12] Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware*. Retrieved from www.cse.psu.edu

[13] Salkind, N. J. (2004). Statistics for people who (think they) hate statistics. Retrieved from http://search.barnesandnoble.com/Statistics-for-People-Who/Neil-J-Salkind/e/9781412979597/?cm_mmc=AFFILIATES-_-Linkshare-_-je6NUbpObpQ-_-10:1.