Android Anti-Virus Analysis

Rahul Ramachandran, Tae Oh and William Stackpole

***Abstract*—The number of devices running with the Android operating system has been on the rise. By the end of 2012, it will account for nearly half of the world's smartphone market. Along with its growth, the importance of security has also risen. A proportional increase in the number of vulnerabilities is also happening to the extent that there are a limited number of security applications available to protect these devices. The efficacies of these applications have not been empirically established. This paper analyzes some of the security tools written for the Android platform to gauge their effectiveness at mitigating spyware and malware.**

***Index Terms*— Android, Security, Anti-virus, Exploits, Malware, Spyware**

I. Introduction

THE use of smartphones ranges from individual consumers to large enterprises. Used for both personal and professional purpose, smartphones have become the new personal computer. Consistent presence and ease of handling of the device lets you perform most of the operations often done on a personal computer. These mobile devices are being used not only for making calls or for texting purposes, but also for interacting with social networking Websites and sometimes performing sensitive financial transactions. But there is concern about the growing security issues on the Android Operating System. Along with their advantages, smartphones also come with all of the issues that personal computers have such as data exfiltration through infection via viruses, malware and spyware.

This paper analyzes various anti-virus applications available in the Android market for their effectiveness in preventing malware from exploiting an Android-enabled mobile device. A number of anti-virus applications were selected to carry out the research. Two popular spyware applications were also selected to test the anti-virus. Test scenarios were designed to enable the testing to be done in different phases. Effectiveness of each anti-virus selected was recorded and studied. Apart from the test, the data transfer process between the anti-virus, spyware and its base servers was also reviewed. Section II discusses the similarities and differences between security issues on a personal computer and a smartphone. An overview of the Android platform, addressing the architecture and associated security issues, are provided. Section III discusses the use of anti-virus, the security aspects associated with anti-virus applications, and why such an analysis is required. Section IV deals with the methodology and the testing processes carried out in our research. Section V discusses the results of the research conducted. Section VI analyzes the results and findings. Section VII gives a brief introduction on the future work that is to be carried out. Section VIII provides conclusions.

II. Background Information

A. PC vs. Smartphone

There are significant differences between a personal computer and a smartphone. One of the most important factors is the mobility and portability of these devices which makes them a workable replacement for a personal computer. Unlike a personal computer which requires frequent shutdown, smartphones are constantly powered [1]. This makes issues specific to power consumption and processing power more important to consider. A personal computer is not always connected to a network, whereas a smartphone usually is. It uses an independent operating system to run various complex applications. Being always on the mobile and wireless networks, these devices are potentially more exposed and more vulnerable to various attacks such as denial of service (DoS), phishing, etc. [2].

The inclusion of a virtual keyboard [3] allows users to experience the Graphical User Interface of a screen. Support of processor intensive applications differs in use amongst a personal computer or a laptop from a smartphone. Today's smartphones come with high-speed processors providing opportunities for larger and more complex applications to be installed on them. For instance, VMware is developing an entirely new concept called the Mobile Virtualization Platform (MVP) which enables running a virtual environment on a mobile device. This allows a company's IT operation to control the use of company's data on any employees' smartphone. Virtualization of smartphones for organization purposes enables the segregation of personal data from company data, providing the necessary data protection for any confidential or sensitive data [5]. Cloud based services have evolved and are now used extensively in a variety of implementations. Use of the "private cloud" is also on the rise. For example, Ubuntu One is a cloud based service for Ubuntu users and enables any user with an Android, iOS, or Windows-enabled smartphone to download the application and use files that have been shared through the Ubuntu cloud [6].

If a smartphone shares many functions of a personal computer, it also shares the inevitable associated security

issues. As a result smartphones have become more vulnerable to viruses, malware, and spyware. While much research has been done in the area of infrastructure-based computing networks, security for the smartphone is relatively new, one of the main reasons for the increase in exploits on the mobile platform is a result of the fact that most smartphone applications are obtained from untrusted third party providers. Additionally, smartphones are increasingly used for the storage of data through applications such as email clients, and social networking tools. This increases the likelihood of attacks on a mobile device [7].

B. What About Android?

The Android OS has come quite a long way since its introduction in 2008 with the HTC G1 [8], Google has named these OS versions in alphabetical order. Astro and Bender were the names dubbed for pre-release versions. Table I shows different version names and their corresponding version numbers [9].

TABLE I
ANDROID VERSIONS

OS Name	Version No.
Ice Cream Sandwich	4.0.x
Honeycomb	3.x.x
Gingerbread	2.3.x
Froyo	2.2
Éclair	2.1
Donut	1.6
Cupcake	1.5

Significant updates to the operating system were made in each successive version. The first version included features such as a web browser, camera support, Gmail sync, Gtalk, etc. in addition to the basic features of a cell phone. Additional features were added in follow-on versions. The Android Market is a cloud-based repository of applications that can be downloaded on to a device. It has over 400,000 applications that number more than 10 billion downloads [10].

C. Understand the Architecture

Major components of the Android architecture are Kernel, Libraries, Application Framework, and Application.

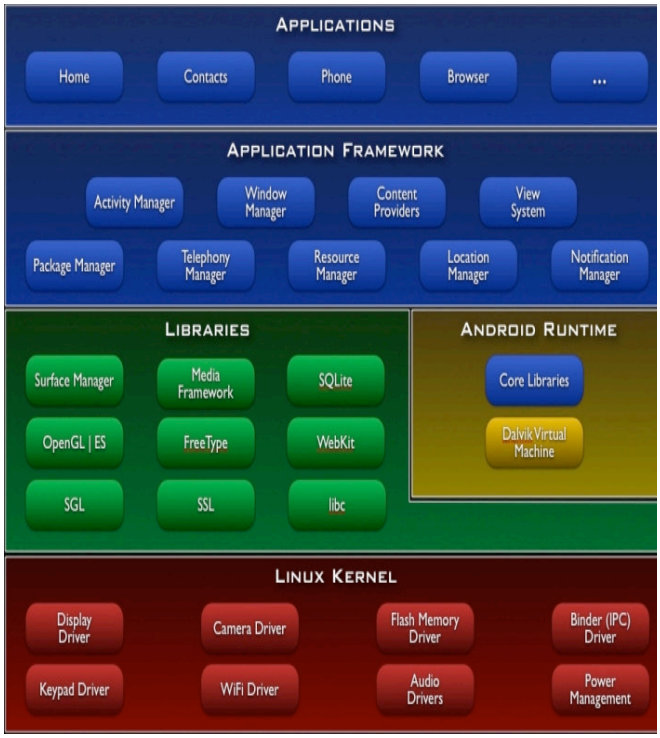

Fig. 1. Android Architecture

Fig. 1 shows the basic Android Architecture [11]. The base stack is the Kernel of the system which acts as an abstraction layer between the hardware and the software stack. It includes memory management, process management, network stack, and driver models.

The next level of the system includes the libraries, which are a set of instructions for handling different kinds of data. These include a set of C/C++ libraries which includes core libraries including the System C library, media libraries, and LibWebCore (for a Web browser engine). For example, media entities like audio, video, and pictures are handled by the media framework library. The Android Runtime layer includes a set of core Java libraries. Android applications are developed using the Java programming language.

The Application Framework includes programs that manage the device's basic functions like navigation, telephone, and resource allocation. Android application developers have access to the application framework which allows them to use the device's processing capabilities and build programs based on it. The Application stack is the user interface where the user interacts with the device.

D. Security Issues

The security issues associated with the smartphone are seeing rapid growth as the popularity of the Smartphone market grows. Anti-malware product providers are working to monetize this market segment. Leading computer anti-virus manufactures have already invested heavily in developing security applications for smartphones. Some of the most popular smartphone operating systems include Android by Google, iOS from Apple, BlackBerry OS from RIM, and Symbian from Nokia.

Android, with a commanding 52 percent of the worldwide

smartphone market [12] currently has the highest potential pay- off for malware developers. Some factors that help to provide such a payoff in the areas of malware on this platform include:

1) Multiple Vendors

Google depends on vendors to deploy updates to the Android OS [13], which are critical for fixing holes in the operating system. Mobile phone manufactures around the globe are using Google's Android Operating System to manufacture their products. Some popular vendors include Samsung, HTC, LG, and Motorola. These vendors have custom designed ROM (Read Only Memory) chips for their devices. Just like patches and updates for a computer software application, the Android operating system will have to be updated and patched for holes and error periodically. Like any other software, Android has evolved through versions of its own. As new and updated versions of Android hit the market, manufactures shift to the newer version for their devices, thereby devices using older version are given less importance. Patches and updates for the older versions are not sent out, allowing potential existing exploits to be utilized to a greater extent.

2) No Application Evaluation

Unlike Apple's app store evaluation process, Google does not evaluate the apps in the Android Market [14] before they are published. Android applications are not limited to sale only on the Android Market – they are also sold on various external sites like "moovv.com" and "samsunggalaxy-s.ru", insulating them from potential oversight. This lack of visibility by Google or the device vendors leave the susceptible to a variety of security issues. Applications from outside the market are high in probability to contain malware and open holes for different spyware applications to get access to the device.

3) Open Source Code

To avoid a central point of failure, Android was released as open source. This was to enable all industry players the freedom to customize Android to their needs. Android's kernel, a Linux-based kernel which runs on the General Public License (GPL) is under the open source Apache Software License (ASL) 2.0. The Android kernel inherits few of the main security features of the Linux kernel. Some of which are: Security at OS level, mandatory application sandbox for all its applications [2], secure inter-process communication, and application defined and user-granted permissions [4]. But there are holes in security features it provides. For instance, all applications need the user to grant permission to perform some functions, but these applications do not show "why" they need certain permissions. Most users blindly allow all permissions that an application requests, with no thought given to the implications of such a decision. This makes the device more vulnerable and provides a backdoor for hackers to exploit the device. Although open source code provides an edge over other platforms, it can also increase the vulnerabilities in the platform.

4) Rooting

An Android-enabled device can be rooted [15], the process by which a user can obtain the root privileges (also called the Super User) of the device. A rooted device will be loaded with a customized firmware version. For example, CyanogenMod is an open firmware based on Google Android's official release [16]. This customized firmware will have the original source code and few third party programs to support features not offered by the official release.

The process of rooting an Android phone is different on phones from different vendors. For instance, rooting an HTC phone involves a process which will turn off the security on the device (S-OFF). The default S-On (Security On) must be turned off in-order to gain the device's write permission [17]. S-Off will unlock the NAND (flash memory) portion and make it writable. Two tools available to root HTC Android phones are "unrevoked" and "Alpharev." Root permission provides the user with the required privileges to interact directly with the operating system. Also, there are various applications available in the market for a rooted device such as "CPU Tuner" and "AutoKiller Memory Optimizer", which allow the user to fine tune the operating system and

possibly improve its performance. This may increase the vulnerability of the device to spyware and other malware. When spyware gains access to a device with root permissions, it can steal all the information from the device with no restrictions.

III. ANTI-VIRUS FOR ANDROID

It was thought at first that smartphones were immune to viruses and malware until Android was broken in 2010. A survey shows the amount of malware identified on the Android platform has increased about 472% during the period June 2011 to November 2011. This survey also goes on to say that 55% of the identified malware was from applications that were installed on the mobile device and 44% were SMS Trojan horses [18]. This increases the value of an anti-virus application. Anti-virus and anti-spyware applications have been in the PC market for years. Now as the mobile market grows, anti-virus manufactures are making their way into the Android market too. Many of the top PC anti-virus manufactures have a mobile version available. The anti-virus market specific to Android is huge given the high probability of any given Android-enabled mobile device's falling to vulnerabilities.

Anti-virus tools for smartphones provide features similar to those written for non-mobile computers. Along with offering virus, malware, and spyware protection, they also provide various other features such as back-up of the phone's data, remote erasing of the phone's data, and finding the phone if it is lost or misplaced. There are various free anti-virus applications available for the Android platform including Lookout Mobile security, AVG Free, and Anti-virus free which provide all the basic protection an android-enabled device needs. There are also paid versions of these applications which offer enhanced support and additional

features for the user.

Does the use of Anti-Virus really protect the device? The answer is yes, it does but only to a certain extent. But to what extent the anti-virus works would remain questionable. The research revealed varying results, from which the effectiveness of the use of Anti-Virus applications was deduced. But do these applications provide full protection? The answer appears to be no. Just like new computer malware are generated every day, malware for mobile platforms are on the rise.

Even though the effectiveness of the anti-virus applications remains in question, it is advisable to use it to reduce the probability of an exploit. Anti-virus applications are updated to block frequently spread malware. Apart from providing protection they provide various other features like remote locking, device location, and remote content wiping which can prove to be useful under extreme circumstances. For instance, if someone accidently loses their mobile phone with confidential information in it, it could be possible for the user to remotely wipe out the contents of the phone, while also using the phone finder to locate the device. However the task of choosing an anti-virus system will be challenging given the number of options.

Why Anti-Virus Analysis?

As information is becoming pervasive on smartphones, there is a need to understand the mobile operating system and associated security issues. Many anti-virus and malware prevention tools were found in the Android Market, each claiming to fully protect the device. In computer terms anti-virus works in two ways: behavior-based detection and signature-based detection. Most of the Anti-Virus applications' signatures are updated only after a significant, vendor-detected event that has led to data exfiltration. Anti-Virus analysis seems to be necessary as there does not appear to be independent evaluations of the quality or efficacy of anti-virus tools.

IV. Methodology

Various questions were considered at the beginning of the research. First and foremost, "can the anti-virus detect a suspicious application?'

Another problem considered was the efficiency of any anti-virus application in protecting a given Android-enabled smartphone.

A. Questions

In this security assessment the authors, wanted to address the following two questions,

Question 1: Will the spyware be detected if it precedes the installation of the anti-virus?

Question 2: Will the spyware be detected if it's installation follows the installation of the given anti-virus tool?

B. Criteria

There are several anti-virus and anti-malware applications present for the Android operating system. The authors decided to analyze a few of the top applications based on certain criteria. A detailed search was conducted on the current number of applications available in the Android market and from third party mobile application developers. One of the main criteria considered was the rating given to each application in the Android market [19]. Another criteria was the number of downloads of each applications. This was used as a metric to evaluate the popularity and the quality of the application. Reviews from various online magazines and journals were also considered for the selection. However, performing reverse engineering on these applications was not performed to ensure that the End User License Agreement (EULA) was not violated. Based on these a list of six applications was prepared which would be tested. Similarly, two spyware applications were chosen based on the reviews and popularity. Few of these commercial applications provide the user with a Web page to view all extracted data from the smartphone. To ensure that the tenets of responsible disclosure were followed, the specific names and versions of the anti-virus and spyware tools have been omitted from this report. The anti-virus tools will be referred to as AV* and the spyware tools as SA*.

C. Test Conditions

The tests were carried out on three Android-enabled smartphones LG Optimus V, Samsung Galaxy Nexus, and HTC Wildfire. The reason for selection of these phones was to include in our study both CDMA and GSM mobile phones. The tools were tested directly on the physical devices. The LG Optimus V was a CDMA device from Virgin Mobile, the Samsung Galaxy Nexus was a GSM device with an AT&T connection, and the HTC Wildfire with an AT&T connection was rooted and running on the Cyanogen Android firmware. All the devices were wiped of information (factory reset) prior to testing to ensure a consistent starting point. All selected spyware tools provided a view of infiltrated data through a web-based interface.

D. Test Scenario

To address the questions listed in the section IV. A. the following two scenarios were considered:

Scenario 1: *Install the spyware followed by the anti-spyware application.*

Scenario 2: *Install the anti-spyware application followed by the spyware.*

Each test scenario had several test cases designed to test each of the anti-virus applications against the spyware applications.

E. Test Procedure – Examine

The following procedure was carried out on the test device each time a spyware was installed for testing:

- Incoming and outgoing calls were made
- SMSs were sent and received

- Contacts were added and deleted
- Websites were browsed
- Bookmarks were added and deleted
- Pictures were taken and deleted.
- Web portal of the spyware was checked to determine the modified data

F. Test Execution

For all test scenarios, the unit under test was formatted and returned to a "factory default" state prior to the start of each scenario. In the first scenario, the selected spyware was installed on the test device. On this unprotected device, the *Examine* procedure was carried out. In all cases the spyware was successfully able to update, the extracted data from the infected device. This step was followed by the installation of the anti-virus application. A full system scan was performed on the test device to detect the installed spyware. The software under test was deemed to be successful if it detected the installed spyware. If the anti-virus application was detected, the *Examine* procedure was carried out again to prove the inefficiency of the application.

In the second scenario, the anti-virus application was installed on the test device. A full system scan was performed to make sure the application was up and running. On the "protected" device, the spyware was installed and the *Examine* procedure performed. The efficacy of the anti-virus application was checked to determine whether or not it had blocked the installation of spyware. If it had not blocked the installation, the ability of the AV tool to detect and disable the spyware was evaluated. The responses were recorded and results tabulated.

V. Result

The following tables show the results of the tests performed. These tables present our findings/results and our evaluation of the tool's effectiveness. The applications were tested to assess their ability to communicate information about the test device to the server associated with the application. Observations were made on the ability of the anti-virus products to identify, detect, and/or disable the spyware installed on the Android phone.

1) Scenario 1

Table II shows the results of the first test scenario where the spyware was installed before the anti-spyware was added to the device's application list. Names of the anti-virus applications are not disclosed. Identified and Disabled (I&D) mean the anti- virus was able to identify the spyware application as malicious and disable it completely from sharing the device's information with its server. Detected (D) mean the anti-virus was able to detect the spyware as an application that was installed on the device.

TABLE II
ANTI-VIRUS VS. SPYWARE – SCENARIO 1

		Anti-Virus					
		AV-1	AV-2	AV-3	AV-4	AV-5	AV-6
Spyware	SA-1	I&D	D	I&D	D	D	D
	SA-2	I&D	D	I&D	D	D	D

2) Scenario 2

Table III shows the result of the second test scenario where the anti-virus was installed before the device was infected by the spyware. No Action (N) was termed where the anti-virus application failed to detect the spyware as any other application, i.e. it was not detected by the scanner.

TABLE III
ANTI-VIRUS VS. SPYWARE – SCENARIO 2

		Anti-Virus					
		AV-1	AV-2	AV-3	AV-4	AV-5	AV-6
Spyware	SA-1	I&D	N	I&D	N	N	N
	SA-2	I&D	N	I&D	N	N	N

3) Anti-Virus/Spyware Operation

There are a few approaches to examine how spyware and anti-spyware share information with their server(s). One way is to check the source code of the application to determine its function. Another is to use a terminal application to watch for communication to and from the applications. The "netstat" command, which displays protocol statistics and current TCP/IP connections, was used in the "Connect Bot" (Secure Shell client) application to identify open connections on the phone. This command was executed before and after the applications was installed. This process was also performed with the anti-virus and the spyware application. The findings show that many applications open a port on the test device to establish an http or https connection with their respective server to transfer the data. Fig. 2 shows the snapshot of one of the anti-virus applications opening a TCP connection. Fig. 3 is the snapshot of one of the spyware applications establishing a connection. Few of the anti-virus and spyware did not appear to be running in the connections.

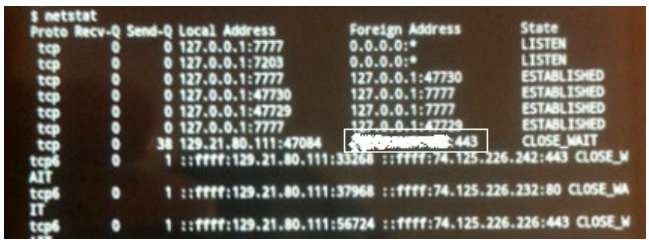

Fig. 2. Anti-Virus snapshot of 'netstat' command

Fig. 3. Spyware snapshot of 'netstat' command

VI. Analysis

The expectation of this research was to test the effectiveness of the current anti-virus applications available for the Android platform. There were various factors which were not considered. For instance, some spyware operates like a Trojan horse, covertly stealing data from the infected device. Similarly, the "Connect Bot" application or the "netstat" command could have been compromised. The authors believe this to be unlikely, given that the devices were returned to a 'known-good' state before each successive test cycle. Another factor was the effectiveness of the spyware operation. Spyware was not tested nor expected to perform consistently. Hence multiple attempts were made to make sure consistent results showed up. One other factor was the version of the Android operating system. Testing was performed on three devices without considering the version number of the Android. All the anti-virus applications tested were free versions from the Android market.

From the research performed it can be said that not all anti-virus applications are effective at preventing malware and spyware from infecting an Android phone. Out of the six anti-virus applications tested, only two were able to detect both the spyware exploits. The other anti-virus applications appeared to have failed at detecting or mitigating the data exfiltration process. Just 30% of the applications chosen were able to detect spyware installed or being installed. Considering the number of Android phones out in the market, the collection of available security tools appears to be very limited. The applications tested, showed similar operations and performance on both CDMA and GSM phones.

VII. Future Work

This ongoing research focuses on the behavior of anti-virus and spyware applications and their operations. Based on the behavior, a new strategy can be designed for developing an anti-virus to give smartphones maximum protection. Future work will emphasize on regression testing of already tested anti-virus applications to deduce the behavior of their performance, testing of other major anti-virus applications in the Android Market, and other testing to discover additional mobile device vulnerabilities.

VIII. Conclusion

The paper discussed the android architecture along with the various security issues covering rooting, anti-virus and spyware among others. A clear analysis has been attempted using various test scenarios. It also discussed the efficiency of anti- virus applications available for the Android operating system.

Based on the research it can be concluded that the Android operating system has a high potential to susceptibility of spyware and other malware. The security applications tested on the Android platform are weak. There remains a need for effective anti-virus and anti-spyware applications that accurately detect and mitigate data exfiltration events. Having a stronger set of such tools would provide availability of better anti-malware protection to all users of Android-based devices.

References

[1] Miller, C.; Mobile Attacks and Defense, Security & Privacy, IEEE, July-Aug. 2011, pages 68 - 70
[2] Bläsing, T.; Batyuk, L.; Schmidt, A.-D.; Camtepe, S.A.; Albayrak, S.; - An Android Application Sandbox System for Suspicious Software Detection. Malicious and Unwanted Software (MALWARE), 5th International Conference, pages 55 - 62. IEEE 2010
[3] Sarcar, S. ; Ghosh, S. ; Saha, P.K. ; Samanta, D. - Virtual keyboard design: State of the arts and research issues. Students' Technology Symposium (TechSym), 2010 IEEE
[4] Android Security. [Online]. Available: http://source.android.com/tech/security/index.html
[5] Forbes Video Network – Intelligent Technology, [Online]. Available: http://video.forbes.com/fvn/future-tech/vmware-virtual-smartphone
[6] Ubuntu One, [Online]. Available: https://one.ubuntu.com/
[7] Delac, G. ; Silic, M. ; Krolo, J. ; Emerging security threats for mobile platforms - MIPRO, 2011 Proceedings of the 34th International Convention, pages 1468-1473, July 2011
[8] Kent German. (2011, August 2). CNET - A brief history of Android phones, [Online]. Available: http://reviews.cnet.com/8301-19736_7-20016542-251/a-brief- history-of-android-phones/
[9] Platform Versions, Android Developers, [Online]. Available: http://developer.android.com/resources/dashboard/platform-versions.html
[10] Don Reisinger. (2012, January 4). Android Market hits 400,000 available apps, says analytics firm, [Online]. Available: http://news.cnet.com/8301-13506_3-57351969-17/android- market-hits-400000-available-apps-says-analytics-firm/
[11] What is Android? Android Developers [Online] Available: http://developer.android.com/guide/basics/what-is-android.html
[12] Charles Arthur. (2011, November 15). Android runs 52% of smartphones sold, [Online] Available: http://www.guardian.co.uk/technology/2011/nov/15/android-runs-most-smatphones-sold
[13] Alexking.org. [2011, March 9]. The Android OS Update Problem, [Online] Available: http://alexking.org/blog/2011/03/08/android-os-update-problem
[14] Publishing process | Android, Amazon Mobile, [Online] Available: http://kb2.adobe.com/cps/900/cpsid_90052.html
[15] Robert Strohmeyer. PCWorld.com. (2010, September 14). Root Android the Easy Way, [Online] Available: http://www.pcworld.com/businesscenter/article/205336/root_android_the_easy_way.html
[16] CyanogenMod, [Online] Available: http://www.cyanogenmod.com
[17] XDA-Developers. (2011, June 28). Rooting HTC Wildfire, [Online] Available: http://forum.xda-developers.com/showthread.php?t=1145035
[18] David Court. (2011, November 18). PC Advisor - Do I need antivirus software for my smartphone, [Online] Available: http://www.pcadvisor.co.uk/features/security/3319310/do-i- need-antivirus-software-for-my-smartphone/
[19] Android Market [Online] Available: https://market.android.com/