Think India Journal
ISSN: 0971-1260Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

Android Smartphone Defining Malware Attack and Security

Indumathy R,&
Nagaraj K,
Assistant Professor,
Dept. of Computer Science,
Vel Tech RangaSanku Arts College

ABSTRACT

Like a computer RAM, RAM in Android is essential for multitasking especially on Android OS, Android has great multitasking feature built into it. Bigger the RAM size fasterthe accessing speed of your Android phone apps, games &files.

Latest Android Phones available with inbuilt RAM between 512 MB to 2 GB depending uponyourphone.Ifyouhaveanylatestphonewithdualcoreprocessorthenchancesareyouhave 2 GB of RAM. Unfortunately most of the people have starting range Android phone which has 512 MB to 1 GBRAM.

Although 512 MB of RAM might be sufficient for daily use, but you must have noticed that your Android Phone slowing down by the end of the day or especially when you launch a new app after long time browsing web pages, it make your app super slow until you restart it again.

In this we will share Apps To Increase RAM Speed of Android Phones. Ideally it is not possible as RAM is allocated within the internal memory of Android device, but there are some third party Apps those can allocate the RAM to your SD card instead of your Phone's internal memory, thus this way you can increase your RAM up to4GB.

In this project we used java eclipse to make android more and most effective.Hence the emulator setup make the prolonged retension of battery and mobile life.

INTRODUCTION

The use of smart phones ranges from individual consumers to large enterprises. Used for both personaland professional purpose, smart phones have become the newpersonal computer. Consistent presence and ease of handling of the device lets you perform most of the operations oftendoneonapersonalcomputer.Thesemobiledevicesarebeingusednotonlyformakingcalls or for texting purposes, but also forinteracting with social networking Websites and sometimes performingsensitivefinancialtransactions.Butthereisconcernaboutthegrowingsecurityissues on theAndroid OperatingSystem.

Along with their advantages, smartphones also come with all of the issues that personalcomputers 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 weredesignedtoenablethetestingtobedoneindifferentphases.Effectivenessofeachanti-virus selected was recorded and studied. Apart from the test, the data transfer process between theanti- virus, spyware and its base servers was also reviewed. Section II discusses the similarities and differences between security issues on a personal computer and asmartphone.

An overview of the Android platform, addressing the architecture and associated security issues,areprovided.SectionIIIdiscussestheuseofanti-virus,thesecurityaspectsassociatedwith antivirus 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 carriedout.

THEORETICAL FRAMEWORK

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].

Thismakesissuesspecifictopowerconsumptionandprocessingpowermore importantto consider.Apersonalcomputerisnotalwaysconnectedtoanetwork,whereasasmartphoneusually is. It uses an independent operating system to run various complexapplications.

Being always on the mobile and wireless networks, these devices are potentially more exposedandmorevulnerabletovariousattackssuchasdenialofservice(DoS),phishing,etc.[2]. The inclusion of a virtual keyboard [3] allows users to experience the Graphical User Interfaceofa 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.

EXISITING SYSTEMS

Smartphonemalwarehasbecomearatherprofitablebusinessduetotheexistenceofalarge number of potential targets and the availability of reuse-oriented malware development methodologies that make exceedingly easy to produce newsamples.

Smartphonemalwareisbecomingincreasinglystealthyandrecentspecimesarerelyingon advanced code obfuscation techniques to evade detection by securityanalysts.

More sophisticated obfuscation techniques, particularly in code, are starting tomaterialize (e.g., stegomalware). These techniques and trends create an additional obstacle to malware analysts, who see their task further complicated and have to ultimately rely on carefully controlled dynamic analysis techniques to detect the presence of potentially dangerous piecesof code.

DISADVANTAGE

Obfuscation resilient detection is based on semantics rather than syntax.

RESEARCH OBJECTIVES

In this paper we describe ALTERDROID, a tool for detecting, through reverse engineering,

Think India Journal
ISSN: 0971-1260Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

obfuscatedfunctionalityincomponentsdistributedaspartsofanapppackage.Suchcomponents are often part of a malicious app and are hidden outside its main code components (e.g. within data objects), as code components may be subject to static analysis by marketoperators.

The key idea in ALTERDROID consists of analyzing the behavioral differences between the original app and an altered version where a number of modifications (faults) have been carefully introduced. Such modifications are designed to have no observable effect on the app execution,providedthatthealteredcomponentisactuallywhatitshouldbe(i.e.,itdoesnothide any unwantedfunctionality).

For example, replacing the value of some pixels in a picture or a few characters in astring encoding an error message should not affect the execution. However, if after doing so it is observedthatadynamicclassloadingactioncrashesoranetworkconnectiondoes nottakeplace, it may well be that the picture was actually a piece of code or the string a network address or a URL.

ADVANTAGES

ALTERDROID is designed and built to allow ease of tailoring and flexibility in functionality.

We provide simple yet powerful enough models for fault injection operators, behavioral signatures and rule-based analysis of differentialbehavior.

SCOPE OF THE RESEARCH

Scope of the project is to impliment the app process virus scan,boosting and blockingup the unwanted apps in the single app process and to increase the android phone performance and also to increase the speed and space management of the phone.

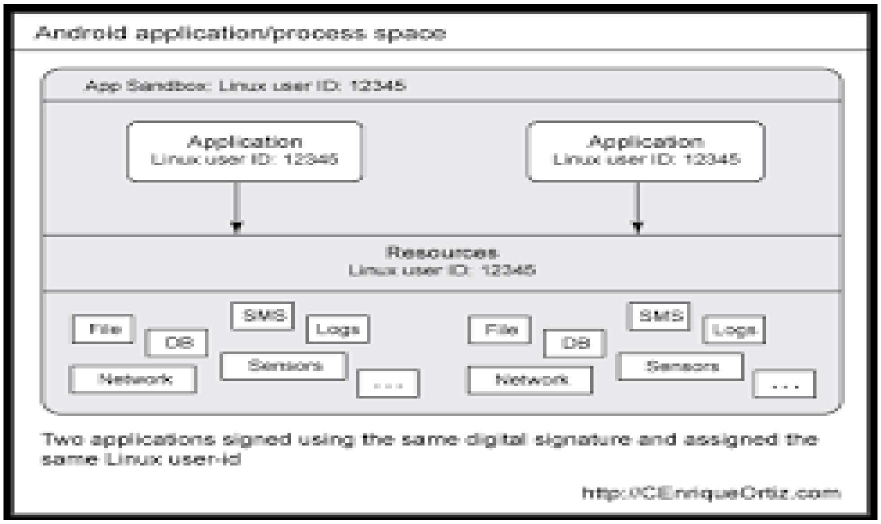
METHODOLOGY

SIGNATURE

Declares a security permission that can be used to limit access to specific components or

Think India Journal
ISSN: 0971-1260Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

features of this or other applications. See the permission section in the introduction, and the Security and Permissions document for more information on how permissionswork.



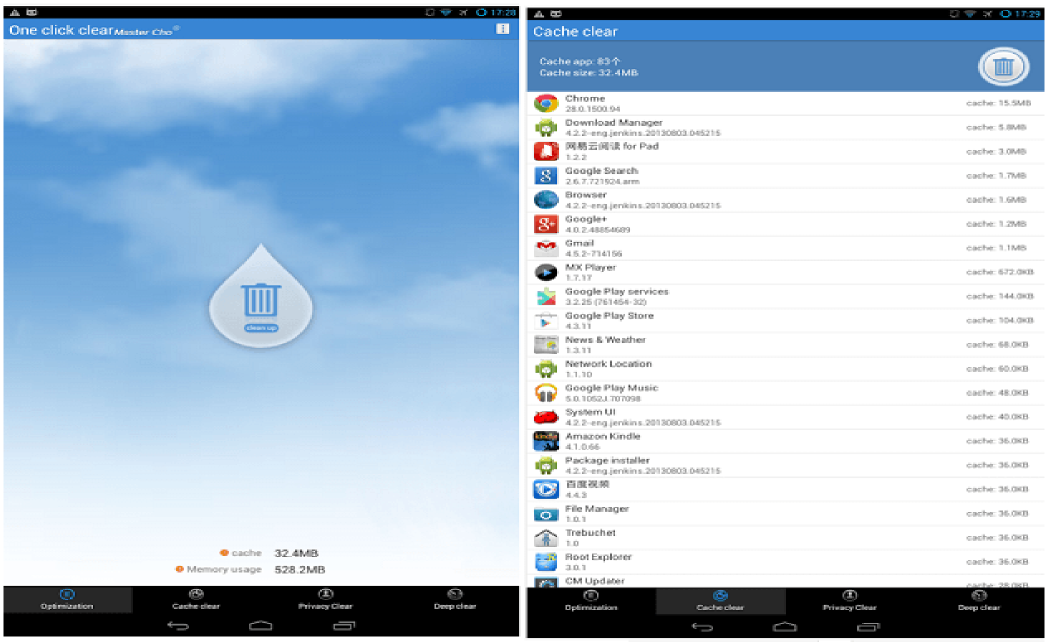
VIRUS SCAN

A type of antivirus program that searches a system for virus signatures that have attached to executable programs and applications such as e-mail clients. A virus scanner can either search all executables when a system is booted or scan a file only when a change is made to the file as viruses will change the data in afile.

Think India Journal
ISSN: 0971-1260Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

CATCH THE MEMORY CLEANUP

An app on your **Android** phone has suddenly stopped working correctly and relaunching the app didn't help, clearing the app **caches** may get things working properly again. To start, pop



open your phone's Settings app. Scroll down and tap Apps under the Device heading.

BLOCKING OF UNWANTED APP

As we are all aware that Android being an open source platform has many benefits, such ascustomizationandunlimitednumberofapps.Butmostofusdon'tthinkaboutthedisadvantages of it. There can be many malware installed on your device right now and the user might not be aware of it. One of the major problems which can be seen right now is that unwanted apps are getting downloaded automatically on your Smartphone, without a user's permission. Well Folks, donotworry,herearesometipsandtrickonhowtostopthemfromgettinginstalledautomatically on your device. Do take a look and keep your smart phone safe and in goodhands.

Think India Journal
ISSN: 0971-1260Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

SPEEDUP CHECK

Automatically increases the speed and check the speed with default and manually using bosst app inbuilt.

CONCLUSION

The paper discussed the android architecture along with the various security issues coveringrooting,anti-virusandspywareamongothers.Aclearanalysishasbeenattempted 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 systemhasahighpotentialtosusceptibilityofspywareandothermalware.Thesecurityapplicationsteste dontheAndroidplatformareweak.Thereremainsaneedforeffectiveanti-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-malwareprotection

Think India Journal
ISSN: 0971-1260Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

FUTURE ENHANCEMENTS

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-virustogivesmartphonesmaximumprotection.Futureworkwillemphasizeonregressiontesting 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 discoveradditional mobile devicevulnerabilities.

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 withoutconsideringtheversionnumberoftheAndroid.Alltheanti-virusapplicationstestedwere free versions from the Android market. From the research performed it can be said that not all antivirus applications are effective at preventing malware and spyware from infecting anAndroid phone.

Out of the six antivirus applications tested, only two were able to detect both thespyware exploits.Theotheranti-virusapplicationsappearedtohavefailedatdetectingormitigatingthedataexfiltrationprocess.Just30% oftheapplicationschosenwereabletodetectspywareinstalled or beinginstalled.

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 on to all users of Android-based devices

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.

[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 onInformation 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 for296295291smartphones 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.

[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.