International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 3 41 - 45

# Andro-Shield

Pratik R. Kaware
Department of Computer Science and Engineering, Datta Meghe Institute of Engineering and Technology, Wardha, India
*2401pratik@gmail.com*

Akshay Vihirkar
Department of Computer Science and Engineering, Datta Meghe Institute of Engineering and Technology, Wardha, India
*akshayvihirkar@gmail.com*

Vaishnavi P. Mapari
Department of Computer Science and Engineering, Datta Meghe Institute of Engineering and Technology, Wardha, India
*vaishnaviamapari@gmail.com*

Parag R. Vitonde
Department of Computer Science and Engineering, Datta Meghe Institute of Engineering and Technology, Wardha, India
*vparag399@gmail.com*

Sanket Daburkar
Department of Computer Science and Engineering, Datta Meghe Institute of Engineering and Technology, Wardha, India
*sanketdaburkar@gmail.com*

Guided By - Asst. Prof. Kapil Gupta
Prof. Department of Computer Science and Engineering, Datta Meghe Institute of Engineering and Technology, Wardha, India
*kaps04gupta@gmail.com*

***Abstract:*** Today Android has the biggest market share as compared to other operating system for smart phone. As users are continuously increasing day by day the Security is one of the main concerns for Smartphone users. As the features and power of Smartphone are increase, so that they have their vulnerability for attacks by Malwares. But the android is the operating system which is more secure than any other operating systems available for Smart phones. The Android operating system has very few restrictions for developers and it will increase the security risk for end users. I am proposing an android application which is able to perform dynamic analysis on android program. To perform this analysis,I have to deploy the android application, in this proposed system I am going to deploy android application on a local server. This application executes automatically without any human interaction. It automatically detects malware by using pattern matching algorithm. If malware get detected, then user get inform that particular application is malicious and restrict the user from installing application.

***Keyword:*** *Android, vulnerability, malwares, smart phones*

*****

## I . INTRODUCTION

Smartphones have become omnipresent devices. Theycombine the computing power previously known from desktop computers with the mobility and connectivity of cellularphones. With their plethora of interfaces like Bluetooth,Wifi, and the cellular network they remain connected tothe Internet at all times.The smart phone devices are uses in a range of individual to large enterprises. It will be use for both personal and professional purpose smart phones have become the new personal computer. Consistent performance and ease of handling of the device lets you perform most of the operations often done on a Pc's. These mobile devices are being used not only for just making calls or messaging, but also for interacting with social networking Websites and sometimes performing sensitive financial transactions. There are many operating systems available for the smart phones, one of this is The Android operating system. Android is a modern mobile platform which is designed to be truly open source. The Android applications can use advanced level of both hardware and software as well as local and server data, through this platform developer bring innovation and value to consumers. Android platform must have security mechanism to ensure security of user data, information, application and network [1]. To provide security in Open source platform needs strong and rigorous security architecture. The Android is designed with multi-layered security which will provides flexibleness needed by an open source, whereas providing protection for all users of the platform designed to a software stack android includes a middleware and core application as a complete [2]. Android architecture is designed with keep ease of development ability for developers. The Security controls have designed to minimize the load on developers. The Developers have to simply work on versatile security controls because developers are not familiar with securities that apply by defaults on applications.Much malware today is generated with the help of virus generation kits, or areslightly modified copies of already known malware. In practice we find that these malwareinstances often contain some invariant code. By identifying this code, it is possibleto generate a signature that finds all variants of the same malware. Such generic signatureshelp reduce thememory needed to store signatures and speed up the time needed

to scan files.

### A. *Security Issues faced by Android*

Android is not secure as it appears, even when such robust security measures. There are several security problems faced by the android, which are given below:

1. Android has no security scan over the apps being uploaded on its market.
2. There are some apps which can exploit the services of another app without permission request.
3. Android's permission security model provides power to user to make a decision whether an app should be trusted or not.
4. The Open Source is available to legitimate developers as well as hackers too. So that the Android framework cannot be trusted when it comes to develop critical systems.
5. The Android operating system developers clearly state that they are not responsible for the security of external storage.
6. Any app on the android platform will access device data just like the GSM and SIM marketer Ids while not the permission of the user.

### *B. Smartphone Architecture*

Modern smartphones comprise many complex subsystems.The central one is the application processor that runs thesmartphone OS such as Android or iOS and all the applications.Other systems include the baseband, GPS and audiohardware. See Figure 1 for a conceptual hardware layout ofa smartphone.The application processor comes in the form of a Systemon a Chip (SoC). The CPU, memory and interrupt controller,timer as well as additional functional units are integratedon one silicon chip. This design helps to reduce the bill of materials and power usage. Usually the SoC also integratesa graphics processing unit and controllers for system buses such as I2C, SPI and USB. These buses are used to connect peripheral devices.

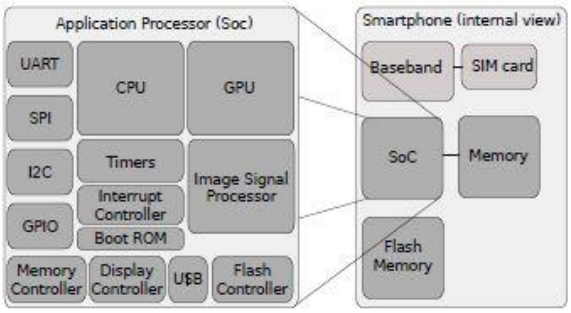


Figure 1: The basic design of a modern smartphone.

## II. LITERATURE SURVEY

B. J. Berger, M. Bunke and K. Sohr presented an android security case study with Bauhaus. In this paper analysis, they discovered that firms and corporation now uses security software for code analysis to discover security problems in application. They carried out a case analysis on android based mobile in cooperation with a security expert and employed the reverse engineering tool-suite Bauhaus for security assessment. During the investigation they found some inconsistencies in the implementation of the Android security concept. Based on the case study, they suggest several research topics in the area of reverse engineering that would support a security analyst during security assessments [3].

H. G. Schmidt, A.D. Schmidt, J. Clausen, A. Camtepe, S. Albayrak, K. Ali Yüksel and O. Kiraz review on "enhancing security of Linux-based android devices". presents an analysis of security mechanism in Android Smart phones with a focus on Linux. Results of their discussion can be applicable for android as well as Linux-based smart phones. They analyzed android structure and the Linux- kernel to check security functions. They also review well accepted security mechanisms and tools which could increase device security. And they provided details on how to adopt these security tools on Android platform and overhead analysis of techniques in terms of resource usage [4].

S. Powar, Dr. B. B. Meshram, review on "Android security framework", Describes android security framework. Raising exposure of open source Smartphone is increasing the security risk. The android provides a basic set of permissions to secure smart phone. The method to make Android security mechanism more versatile and the current security mechanism is too rigid. The user has only two options at the time of application installation first allow all requested permissions and second deny requested permissions leads to stop installation [5].

A. Warg,M. Lange, S. Liebergeld, A. Lackorzynski, M. Peter represented „L4Android: a generic operating system framework for secure smart phones". They present a generic operating system framework that overcomes the need of hardware extensions to provide security in smart phones. They bind smart phone operating system in a virtual machine; this framework allows highly secure applications to run side-by- side with the VM. Which is based on a state-of-the-art micro-kernel that ensures isolation between the virtual machine and secure applications [6].

A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, Yael Weiss, analysis „Andromaly: a behavioral malware detection framework for android devices". The proposed framework realizes a Host- based Malware Detection System that continuously monitors various features and events obtained from the mobile device and apply Machine Learning anomaly detectors to classify the collected data as normal or abnormal. They developed four malicious applications and check Andromaly's ability to detect new malware based on samples of known malware. They evaluated many

combinations of anomaly detection algorithms, feature choice methodologies in order to find out the combination that yields the best performance in detecting new malware on android[7].

T. Luo, H. Hao, W. Du, Y. Wang, and H. Yin work on "attacks on WebView in the android system". Web-View is an important element in android platforms, enabling smart phones and tablet apps to insert a simple but powerful browser. To achieve a much better interaction between apps and their embedded browsers, WebView provides range of APIs, permitting code in apps to invoke the JavaScript code within pages which intercept their events and modify those events. Using these features apps will become customized browsers for their required web applications. Now, within the android market, 86 % of the top twenty most downloaded apps in ten various classes use WebView14. The architecture of WebView changes the landscape of the web particularly from the security viewpoint. Two essential component of the Web's security infrastructure are weakened if Web-View and its APIs are used: The Trusted Computing Base (TCB) at the client aspect and therefore the sandbox protection enforced by browsers. Resulting several attacks may be launched either against apps or by them [8].

G. Dini, F. Martinelli, A. Saracino, and D. Sgandurra, discuss on „MADAM: a multi-level anomaly detector for android malware". In this analysis, MADAM can monitor android at the kernel-level and user-level to notice real malware infections using machine learning techniques to differentiate between normal behaviors and malicious ones. The primary prototype of MADAM is able to notice several real malwares found in the world. The device is not affected by MADAM due to the low range of false positives generated after the training phase [9].

## III.OBJECTIVES

The main objectives of the project are listed below:

- The main purpose of Androshield software is, of course, to protect the smartphone from getting infected by any malwares.
- Create a malware defense system which is more efficient, which consumes less battery
- No need to update the "virus signature database" every now and then.
- Break the chain of fake detection of viruses.
- Creating system which is simple but effective than any other anti-virus present today.
- Creating quality norms, quality testing network and quality guidance systems.
- With this, you can do a thorough scan of the apk file and make sure you aren't infected with anything that might be breaching your security or causing your smartphone to slow down.

## IV.PROBLEM STATEMENT

To provide security in Open source platform needs strong and rigorous security architecture. The integration of technologies into an application certification process requires overcoming logistical and technical challenges. The android provides more security than other mobile phone platforms. Some antivirus companies claim to provide full security but failed to provide it.

- Existing malware detection mechanism are very time consuming process.
- High battery Consumption due to Antivirus Application runs in background.
- There should be a method to detect malware efficiently with less time consumption and that application should use less space.

## V. PROPOSED SYSTEM

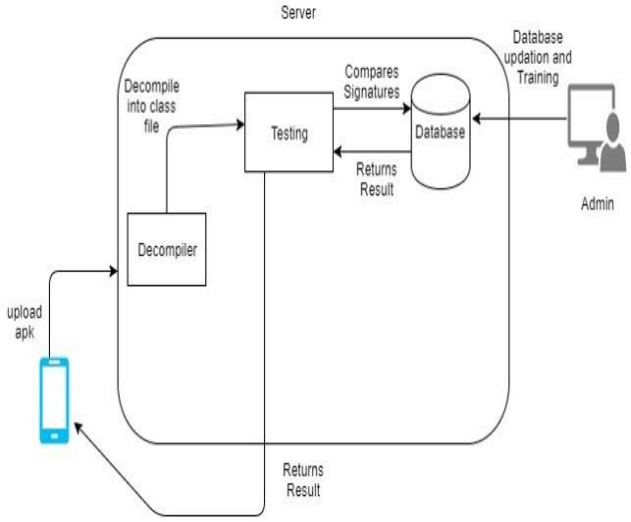


Figure 2: System Architecture

The user will try to install an application to his/her device at that time If the user is an administrator then he/she having an options as training and testing. User has to select the option, if user selects option as training i.e. malware app or spyware or safe app then he/she has to clicks on the upload apk button and select a file for uploading to a local server. then system shows the message that wait while uploading file [10].

Once the file uploaded to the local server, apk file is pass to decompilation app to perform reverse engineering i.e. converts. apk file to java code then it forms the signature which are store in the database [10].

If user want to evaluate the file, then he/she simply select evaluate the .apk and click on upload apk button and select file which we want to check on the local server then it gets decompile first and then perform pattern matching with the signatures present in database once the testing is done user can get the result on his/her android device [10].

**User Interface**

The interface is an android application. The user interface is being kept as simple as possible. Because if we keep the interface simple and efficient it will also attract the user to use the product and it will also help in keeping our promise of using less memory and RAM and as it will be a *lite* version it will also keep battery from draining rapidly. In this tier the multiple user can access the application at a same time but uploading the apk file and its load is totally dependent on server and how efficient the server side machine is.

**DATABASE**

A database is basically a collection of information or records organized in such a way that a computer program can quickly select desired pieces of data. You can think of a database as an electronic filing system. Traditional databases are organized by fields, records, and files. A field is a single piece of information; a record is one complete set of fields; and a file is a collection of records. For example, a telephone book is analogous to a file. It contains a list of records, each of which consists of three fields: name, address.

## VI. METHODOLOGY

1) **Android application for uploading the. apk file on the Server: -**

The first module of a system is an android application which will install on a user's smart Phone. In our System as the apk files are decompile on the local server So, we require to upload apk file on a local server. This application is used to select and upload a apk file to cloud. This Android application provides option like Training and testing once we click on evaluate apk button it will upload a apk file to a local server for the selected purpose.

2) **Android decompiler app on local server: -**

The second module of a system is android decompiler application which is on cloud. This application is used to decompile the apk file which is uploaded by the user via android application. This application convert's apk file to the java file i.e. performs reveres engineering on a APK files.

3) **Training and evaluating app on server**

a) At the time of training we have to select the option training and upload the .apk file on the local server, itgets decompile and form the signatures with the help of decompiler application. We can train our database by adding signature in to the my sql database which is on the local server.

b) At the time of evaluation we have to upload .apk file on local server by selecting a testing option, then app get decompile with the help of decompiler app and match the signatures which are present in the database and gives the answer on the user's smart phone device about the type of the app.

## CONCLUSION

The Proposed System introduced a security service for Smartphone's, which off loads the detection of malicious applications from the Smartphone into the local server. As Smartphone's are very much prone to malwares hence we introduce new approach of using local server as a security weapon for providing security. I proposed a system that detects the malicious code and stores that malware into database which is on the local server and then report to user who wants to installed that application on his / her device.

The Proposed system detects the malicious code from new application and stores the malware in the database of local server. But in future try to make a self-replicate program which will report about malware without database.

## References

[1]. Android Open Source Project. Android Security Overview. http://source.android.com/devices/tech/security/index.html(2013).

[2]. Kaur S. and Kaur M., Review Paper on Implementing Security on Android Application, Journal of Environmental Sciences, Computer Science and Engineering & Technology, 2(3), (2013).

[3]. Berger B.J., Bunke M., and Sohr K., An Android Security Case Study with Bauhaus, Working Conference on Reverse Engineering, 179–183 (2011).

[4]. Schmidt A.D., Schmidt H.G., Clausen J., Camtepe A., Albayrak S. and Yuksel K. Ali and Kiraz O., Enhancing Security of Linux-based Android Devices,http://www.dai-labor.de/fileadmin/files/publications/lk2008-android _security. pdf (2008).

[5]. Powar S., Meshram B. B., Survey on Android Security Framework, International Journal of Engineering Research and Applications, 3(2), (2013).

[6]. Lackorzynski A., Lange M., Warg A., Liebergeld S., Peter M., L4Android: A Generic Operating System Framework for Secure Smartphones, 18th ACM Conference on Computer and Communications Security, 39-50 (2011).

[7]. Shabtai A., Kanonov U., Elovici Y., Glezer C. and Y. Weiss, Andromaly: a behavioural malware detection

framework for android devices, Journal of Intelligent Information Systems, 38(1), 161-190 (2012).

[8]. Luo T., Hao H., Du W., Wang Y. and Yin H., Attacks on WebView in the Android System, 27th Annual Compute Security Applications Conference, 343-352 (2011).

[9]. Dini G., Martinelli F., Saracino A. and Sgandurra D.MADAM: a multi-level anomaly detector for android malware, http://www.iet.unipi.it/g.dini/research/papers/2012-MMM-ANCS.pdf (2012)

[10]. A. A. Dongre, C. J. Shelke " Review of Malware Defense in Mobile Network Using Dynamic Analysis of Android Application." International Journal of Recent and Innovation Trends in Computing and Communication. Volume 2, Issue 11, November 2014