© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Android Malicious Apps Detection and Notification to Prevent Malware Using New Framework

Rohit Sarjerao Raut[1] , Nishita Nitesh Patil [2]

[1]ME Student, Dept. of CSE, Ashokrao Mane Group of Institution vathar tarf vadgaon, Kolhapur, India

[2]Assistant Professor, Dept. of CSE, Ashokrao Mane Group of Institution vathar tarf vadgaon, Kolhapur, India

ABSTRACT

The attractiveness and openness of android makes markets targets for malware attacks and causes number of malware instances original hidden behind the large number of applications that seriously harmful to user privacy and security. Due to the popularity of android operating system and use of internet, android application developers are attracted towards cyber crime. For example, any person sends message to another person using internet to install particular application and that could be malicious. Malware is employed intentionally to cause harm to system by gaining confidential information from the device and modifying file contents. To prevent user privacy and provide security to user data by notifying them about malicious applications SVM with a linear classifier is used to differentiate between benign and malicious applications. For feature extraction and selection Fest tool will be used.

Keywords: SVM, Malicious, feature extraction, Fest.

I. INTRODUCTION

Malware is employed intentionally to cause harm to system by gaining confidential information from the device and modifying file contents[6]. The input for system is android application which can be downloaded from play store or other application market. System will extract features of application which is chosen by user to install. Extracted features will be considered for malware detection. Application will be classified into two types, malicious applications and benign applications. If application is malicious then application will be classified into malware class depending on types of features extracted.

Then system will notify to the user whether given application is malware or not in the form of result and will suggest user to keep that application on device or not. System that detect for android malware that monitors device actions and its interaction with users and running applications by retrieving different groups of features.

The different malwares like SMS Trojan that sends SMS without the user consent and spyware that take piece of information and private data from the mobile device such as IMEI and IMSI, contacts, messages or social network account, account credentials[2]. This data cached by malicious applications is misused by others.

II. METHODS AND MATERIAL

Android application features will be extracted from applications to study behaviour of applications. Features will be extracted from application which is chosen by user to install and those features take into consideration to detect whether application is malware affected or not. Extraction is primary step in which the application from Google play store and other third party market is taken as input to system. The proposed system will extract features of android application to know about application behaviour. For feature extraction and selection Fest [12] tool is used.

Features are extracted from application to detect malwares in application

$$E(x, y) = \sqrt{\sum_{i=0}^{n}(x_i - y_i)^2}$$

xi and yi are the features

Malware detection will take selected features as an input to find out whether given app is malware or not. Also behaviour of application will be checked by considering features extracted. Selected features contributing to the detection and result of this module will be considered for classification. Malware will be detected by considering set of features extracted in the previous phase and the behaviour of application will be analysed based on these features. Different features like GPS based location, read phone state, premium rate will be considered.

The malware detection process will be executed after the feature extraction and before the classification phase. If malware is detected then information of the detected malware and application in which malware is detected is given to the next block for classification purpose.

Classification of the android malware will depend on the behaviour of application and malware detection phase. In classification phase, if the android application is affected by malware, classification will be done based on types of features extracted from the android application.

Application will be classified into two types, malicious applications and benign applications. If application is malicious then application will be classified into malware class depending on types of features extracted. Classification module classifies the application whether it is malware affected depending on previous phase. If application is malware affected then will produce malware is belongs to which class or type. SVM with a linear classifier will be used to differentiate between benign and malicious applications. After classification of application, system will notify user whether application is harmful to user.

Support Vector Machine" (SVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems

Proposed Architecture

Android application features will be extracted from applications to study behaviour of applications. Malware will be detected by considering set of features extracted in the previous phase and the behaviour of application will be analysed based on these features. In classification phase, if the android application is affected by malware, classification will be done based on types of features extracted from the android application. Notification will be given to user after classifying applications into benign app or malware app and the suggestion will be sent to user whether to install android application or not.

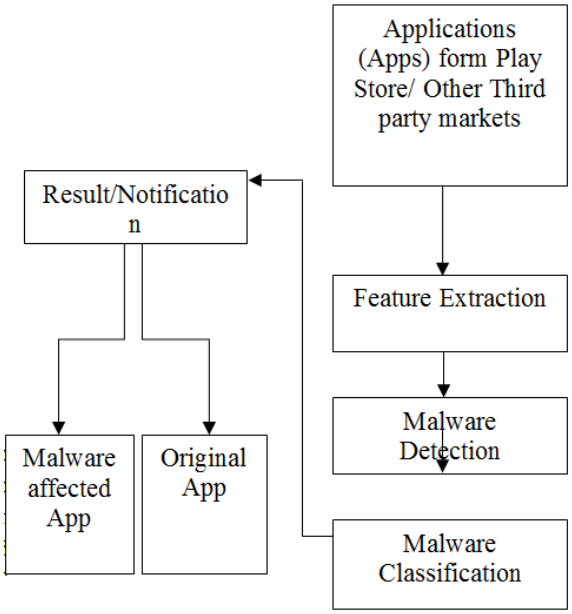
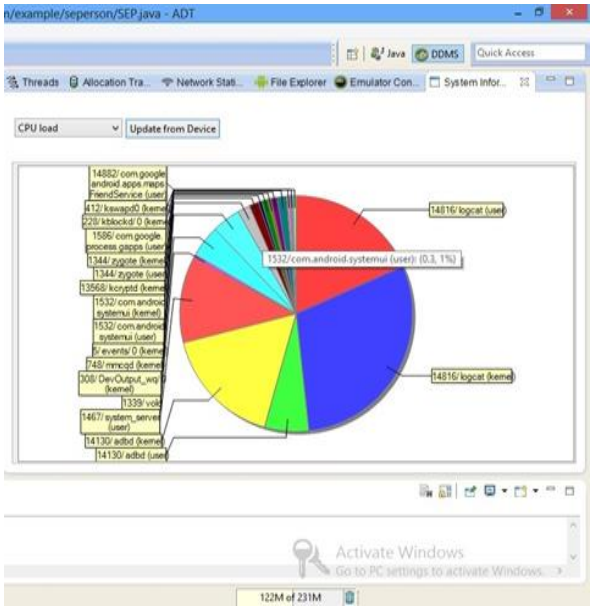


Figure 1. System Architecture

III. RESULTS AND DISCUSSION

The malware detection process will be executed after the feature extraction and before the classification phase. SVM with a linear classifier will be used to differentiate between benign and malicious applications. After classification of application, system will notify user whether



Application to be selected from applist.application is harmful to user. Notification will be given to user after classifying applications into original app or malware app and the suggestion will be sent to user whether to install android application or not.

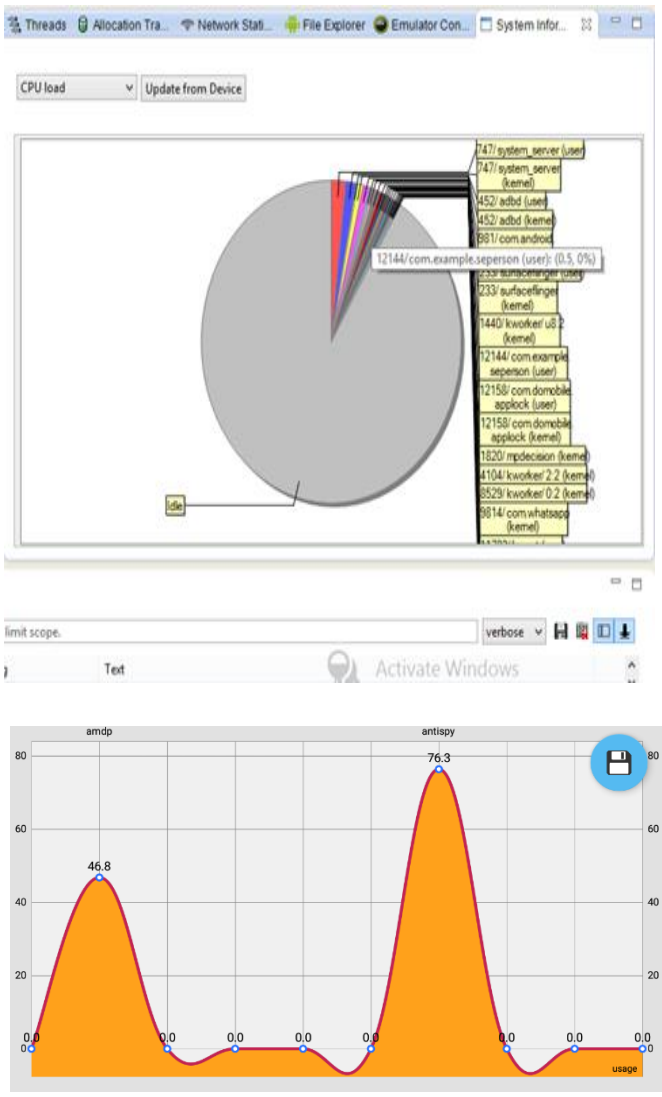


Figure 1 : Memory usage comparison of amdp and antispyware

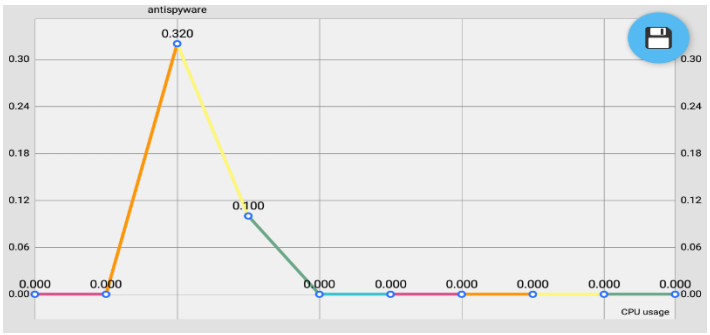


Figure 2 : CPU usage comparison of amdp and antispyware

Three apps considered for compare with amdp, this apps are Trojan, antispy and anti spyware.

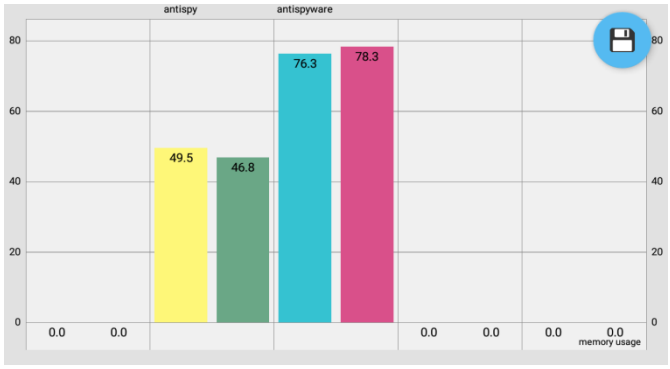


Figure 3 : Memory usage comparison

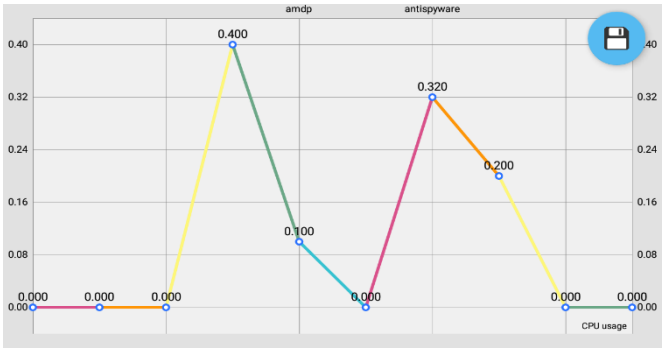


Figure 4 : CPU usage comparison

Implementation Steps:

There are following techniques and algorithm in proposed methodology.

Application features extraction and selection Extraction is primary step in which the application from Google play store and other third party market is taken as input to system. The proposed system will extract features of android application to know about application behaviour. For feature extraction and selection Fest[12] tool will be used. Feature selection improves the accuracy and reduces the False Positive Rate of the classification.

Module 2: Malware detection

Malware detection will take selected features as an input to find out whether given app is malware or not. Also behaviour of application will be checked by considering features extracted. Selected features contributing to the detection and result of this module will be considered for classification.

Module 3: Classification

Classification module classifies the application whether it is malware affected depending on previous phase. If application is malware affected then will produce malware is belongs to which class or type. SVM with a linear classifier will be used to differentiate between benign and malicious applications. After classification of application, system will notify user whether application is harmful to user or not using next module.

Module 4: Notification/ Results

Notification module will take input as classified app from classification phase. This phase will send results to user whether application is benign or malicious and will give suggestions to user about keeping application working is harmful to device and user security

IV. REFERENCES

[1]. Andrea Saracino, Daniele Sgandurra, Gianluca Dini and Fabio Martinelli, "MADAM: Effective and Efficient Behaviour-based Android Malware Detection and Prevention", IEEE Transaction 2016.

[2]. Y. Aafer, W. Du, and H. Yin, "Droidapiminer: Mining apilevel features for robust malware detection in android," inSecurity and Privacy in Communication Networks, Social Informaticsand Telecommunications Engineering, T. Zia, A. Zomaya,V. Varadharajan, and M. Mao, Eds. Springer International publishing, 2013, vol. 127, pp. 86–103. Online]. Available :http://dx.doi.org/10.1007/978-3-319-04283-1 6

[3]. A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. agner,"Android permissions: user attention, comprehension, andbehavior," in Symposium On Usable Privacy and Security, SOUPS'12, Washington, DC, USA – july 11 - 13, 2012, 2012.

[4]. O. Kramer, "Dimensionality reduction by unsupervised k-nearestneighbor regression," in Machine Learning and Applications and Workshops (ICMLA), 2011 10th International Conference on, vol. 1,Dec 2011, pp. 275–278.

[5]. "Global mobile statistics 2014 part a: Mobile subscribers;handset market share; mobile operators," http://mobiforge.com/researchanalysis/ global-obile-statistics-2014-part-a-mobilesubscribers-handset-arket-share- mobile-operators, 2014.

[6]. A.Developer,"Android-sm smanager reference page," 2015.Online]. Available: http://developer. Android .com/reference/ android/telephony/ SmsManager.html

[7]. A. Reina, A. Fattori, and L. Cavallaro, "A system call-centric analysis and stimulation technique to automatically reconstructandroid malware behaviors," EuroSec, April, 2013.

[8]. "How antivirus affect battery life," https://www. luculentsystems.com /techblog/minimize-battery-drain-by-antivirus-software/,last accessed on 23/02/2015.

[9]. Y. Zhou, X. Zhang, X. Jiang, and V. W. Freeh, "Taminginformation- stealing smartphone applications (on android)," inProceedings of the 4th International Conference on Trust andTrustworthy Computing, ser.

[10]. TRUST'11. Berlin, Heidelberg:Springer-Verlag, 2011, pp. 93– 107.online]. Available: http://dl.acm.org/ citation.cfm ?id=20222 45.2022255.

[11]. Y. Zhauniarovich, G. Russello, M. Conti, B. Crispo, and E. enandes, "Moses: Supporting and enforcing security profiles onsmartphones," Dependable and Secure Computing, IEEE Transactionson, vol. 11, no. 3, pp. 211–223, May 2014.

[12]. Y. Zhou and X. Jiang, "Dissecting android malware:Characterization and evolution," in Proceedings of the 2012IEEE Symposium on Security and Privacy, ser. SP '12. Washington,DC, USA: IEEE Computer Society, 2012, pp. 95–109. Online].Available: http://dx .doi.org /10. 1109/SP.2012.16.

[13]. Kai Zhao, Dafang Zhang; Xin Su; Wenjia Li "Fest: A feature extraction and selection tool for Android malware detection", IEEE Symposium on Computers and Communication (ISCC), 2015.