ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on New Enhanced Framework for Android Malware Detection and Prevention

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

ME Student, Dept. of CSE, Ashokrao Mane Group of Institution vathar tarf vadgaon,

Kolhapur, India[1]

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

ABSTRACT: Malicious applications are responsible for misuse of user's private data, 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. This data cached by malicious applications is misused by others. Here we propose a new framework to detect malware in the android applications available over Google play store and other third party markets and prevent user data and privacy by notifying them about malicious applications. SVM with a linear classifier will be used to differentiate between benign and malicious applications. For feature extraction and selection Fest tool will be used.

KEYWORDS: malicious application, fest tool, IMEI, malware

I. INTRODUCTION

Android is popular platform for mobiles and has become extremely famous within last few years. Android dramatically surpassed a billion shipments of its devices and has remained number one mobile operating system.

Google play store and other third party markets play an important role in the popularity of the android devices and any third party vendor can create applications for android phones and deploy it on android markets. Sometimes trusted applications are able to leak user's location and phones identity and share it on server without its consent. Many applications attracted to users to install it by giving wrong information about application. For example, application shows that particular service will start only with internet; no extra charges required but when application being installed the main balance get deducted from mobile.

The openness of android makes these markets hot targets for malware attacks and causes countless instances of malware being hidden behind the large number of benign applications that seriously threatens user security and privacy. Due to the extension growth of android operating system and use of internet, android application developers are attracted towards cybercrime. For example, any person over internet sends message to another person 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. Malicious applications are responsible for misuse of user's private data, 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.

II. LITERATURE SURVEY

A.Saracino, D. Sgandurra, G. Dini, F. Martenelli. [1], presented a novel multi-level and behaviour based, malware detector for Android devices called MADAM (Multi-Level Anomaly Detector for Android Malware). To detect application misbehaviors, MADAM monitored the device actions, its interaction with the user and the running applications, by retrieving five groups of feature sat four different levels of abstraction, namely the kernel level, application-level, user-level and package-level. For some groups of features MADAM applied a signature based approach that considers behavioral patterns known malware misbehaviors.

Author [2] proposed features at API level for malware detection. DroidRange combined permission-based behavioral footprints and a heuristic based filtering scheme to detect malicious applications. Authors overcame the shortcomings of the permission-based warning mechanisms and built a robust and lightweight classifier for Android

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

applications that could be used for malware detection. To select the best features that distinguish between malware from benign applications, API level information within the byte code used. More specifically, they have focused on critical API calls, their package level information.

Author [7] proposed techniques and approaches that behaviors are however achieved through the invocation of system calls; Copper-Droid's VM-based dynamic system call-centric analysis described the behavior of Android malware whether it is initiated from Java, JNI or native code execution. They focused on approach Copper-Droid, an approach built to automatically perform out-of-the-box dynamic behavioral analysis of Android malware; Copper-Droid presented analysis to characterize behaviors.

In this paper authors [9] proposed TISSA model that provided the desired privacy mode on Android by developing an extra permission specification and enforcement layer on the top of existing Android permissions. TISSA consisted of components, first was privacy setting content provider, a privileged component to manage the privacy settings for untrusted applications. It also provided an API that can be used to query the current privacy setting for an installed application.

W. Enck, P. Gilbert. [11], in this paper author proposed new social engineering based technique, Repackaging. It is one of the most common techniques malware authors use to piggyback malicious payloads into popular applications or apps. Malware authors may locate and download popular applications, disassemble them, enclose malicious payloads, and then re-assemble and submit the new applications to official and/or alternative Android Markets. Users could be vulnerable by being enticed to download and install these infected applications.

III. EXISTING SYSTEM

There are already well-known and documented cases of Android malware in both official and unofficial markets. With known malware nefarious capabilities and effects, the detection of malware is an area of major concern not only to the research community but also to the general public. Malware attack is a challenging issue among the Android user community. It therefore becomes necessary to make the platform safe for users by providing defense mechanism especially against malware. The malware detection system available now-a-days like MADAM multilevel anomaly detector for android malware that monitors device actions and its interaction with users and running applications by retrieving different groups of features.

IV. PROPOSED SYSTEM

The proposed system will define a new framework to detect application misbehavior and will add other features like location identity, read phone state, premium rate in the feature extraction technique. The proposed system will be based on enhanced framework of android to detect android malicious applications using different feature sets. The system will include features at user and application level. In addition to these some advanced features will be considered such as GPS based location, read phone state, premium rate.

The proposed system of android malware detection is shown in figure.1. The working of the proposed system is described with following blocks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

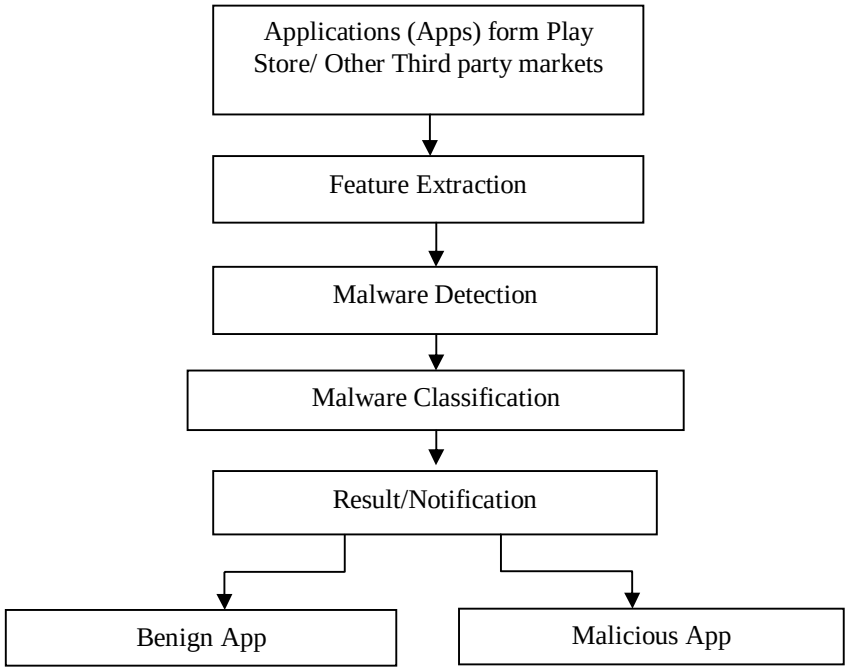

Figure 1: Block diagram of the Enhanced Framework of android malware detection**.**

1 Feature Extraction: -

Android application features will be extracted from applications to study behavior 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. Different features like GPS based location, read phone state, premium rate will be considered. To detect malicious applications, extracted features will be used as input to next step.

2 Malware detection: -

Malware will be detected by considering set of features extracted in the previous phase and the behavior of application will be analyzed based on these features. 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.

3 Classification: -

Classification of the android malware will depend on the behavior 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.

4 Notification: -

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

V.PROPOSED SYSTEM

1 Module 1: 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 behavior. For feature extraction and selection Fest [19] tool will be used. Feature selection improves the accuracy and reduces the False Positive Rate of the classification.

2 Module 2: Malware detection

Malware detection will take selected features as an input to find out whether given app is malware or not. Also behavior 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.

3 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.

4 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.

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 apilevelfeatures 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. Wagner,"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 andWorkshops (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/research-analysis/global-mobile-statistics-2014-part-a-mobilesubscribers-handset-market-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-centricanalysis 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. TRUST'11. Berlin, Heidelberg:Springer-Verlag, 2011, pp. 93–107. [Online]. Available: http://dl.acm.org/citation.cfm?id=2022245.2022255.
[10] Y. Zhauniarovich, G. Russello, M. Conti, B. Crispo, and E. Fernandes,"Moses: Supporting and enforcing security profiles onsmartphones," Dependable and Secure Computing, IEEE Transactionson, vol. 11, no. 3, pp. 211–223, May 2014.
[11] 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.
[12] H. Gascon, F. Yamaguchi, D. Arp, and K. Rieck, "Structuraldetection of android malware using embedded call graphs," inProceedings of the 2013 ACM Workshop on Artificial Intelligence andSecurity, ser. AISec '13. New York, NY, USA: ACM, 2013, pp.45–54. [Online]. Available: http://doi.acm.org/10.1145/2517312.2517315
[13] T. M. Cover, P.E. Hart, "Nearest Neighbor Pattern Classification,"IEEE Transactions on Information Theory, vol. IT-13, no. 1, pp. 21–27,January