IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 12-14
www.iosrjournals.org

Malware Detection in Android App Using Static and Dynamic Analysis

Priyanka Tate[1], Rachana Sonawane[2] , Sagar Shinde[3]
[1]*(Computer Engineering, LogMIEER/ Pune University,india)*
[2]*(Computer Engineering, LogMIEER/ Pune University,india)*
[3]*(Computer Engineering, LogMIEER/ Pune University,india)*

Abstract: *Smartphones and mobile tablets are fast becoming necessary in daily life. Android has been the most popular mobile operating system since 2012. However, due to the open nature of Android, immeasurable malwares are hidden in a large number of kindly apps in Android markets that dangerously pressure Android security. Deep learning is a new area of machine learning research that has gained increasing detect in artificial intelligence. In this study, we propose to connect the features from the static analysis with features from dynamic analysis of Android apps and differentiate malware using deep learning techniques. We execute an Online deep-learning-based Android malware detection engine (DroidDetector) that can automatically identify whether an app is a malware or not. With thousands of Android apps, we systematically test DroidDetector and do an indepth analysis on the features that deep learning basically exploit to differentiate malware. The results show that deep learning is suitable for differenting Android malware and especially useful with the availability of more training data. DroidDetector can get 96.76% detection accuracy, which outperforms traditional machine learning techniques. An estimation of ten popular anti-virus softwares demonstrates the importance of advancing our capabilities in Android malware detection.*

Keywords - *Android security; malware detection; characterization; deep learning; Evaluation.*

I. Introduction

Android harmfully surpassed a billion shipments of its devices in 2014 and has remain the No.1 mobile operating system since 2013, according to a just report from Gartner. Android markets, such as the Google Play Store and other mediator markets, play an important role in the fashion of Android devices. However, the openness of Android makes these markets hot targets for malware attacks and causes countless instances of malware being hidden behind a large number of benign apps that seriously blackmail users' security and privacy. Moreover, a report from McAfee Labs reveals that 3.73 million pieces of mobile malware were identified in 2013, increasing an astounding 197% from the end of 2012 . Accordingly, an urgent need arises to develop powerful solutions for Android malware detection. Unfortunately, the Android market presently has no such solution. Today, the main countermeasure to defense against malware on Android platforms is a risk communication mechanism that calls users about the permissions required before installing each app. This mechanism is rather ineffective as it presents permissions in a Malware Detection in Android App Using Static and Dynamic Analysis 115 complete fashion, thus requiring too much technical knowledge for a user to be able to separate malware from benign apps.

Note that both a benign and a despiteful app may require the same permissions and are thus indistinguishable via this permission-based mechanism. In general, permission-based approaches are developed primarily for risk assessment rather than malware detection.

II. Comparative Study

1. DroidMiner: automatic Mining and classification of Fine-grained Malicious Behaviors in Android Applications. Android app finding approaches rely on yourself selected detection heuristics, features, and models. In this paper, we explain a new, corresponding method, called DroidMiner, which uses static analysis to automatically mine malicious program reason from known Android malware, abstracts this reason into a sequence of threat modalities, and then seeks out these threat modality patterns in other unknown Android apps.

2. DREBIN : efficient and understandable Detection of Android Malware in Your Pocket

Malicious applications pose a threat to the security of the Android stage. The growing quantity and variety of these applications render predictable defenses largely unsuccessful and thus Android smartphones often stay un-protected from original malware. In this paper, we propose D REBIN, a lightweight method for finding of Android malware that allow identifying malicious applications openly on the smartphone. As the limited resources delay monitoring applications at run-time, D REBIN do a large static analysis, gather as many features of an application as possible. These features are fixed in a joint vector space, such that typical patterns problem-solving for malware can be automatically identified and used for explaining the decisions of our way.

3. Android Malware Detection Using Machine Learning Approach we here Permission as well as String Based Anomaly Detection System for detecting Meaningful deviation in a mobile application's network behavior. The main goal of proposed system is to protect mobile device users and avoid uncertainty of users. Identification of republished popular applications injected with a malicious code. More specifically, we attempt to detect a new type of mobile malware with self-updating capabilities that were newly found on the official Google Android Marketplace. Android applications are becoming increasingly because android phones are wide spread and steadily gaining popularity.

4. A Study of Android Malware finding methods and Machine Learning Android OS is one of the widely used mobile Operating Systems. The amount of malicious applications and adware's are increasing constantly on par with the number of mobile devices. A great number of viable signature based tools are available on the market which prevent to an extent the access and distribution of malicious applications. Numerous researches have been conducted which declare that established signature based Finding system work well up to certain level and malware authors use numerous methods to avoid these tools.

5. An review Android Antimalware that identify Malicious Dynamic Code in Apps

Android is currently the most popular operating system and a significant number of Smartphone's, tablet computers ship with Android. However, users feel their personal information at threat, facing a quickly increasing number of malware for Android which significantly exceeds that of other platforms. Antimalware's software guarantee to effectively protect against malware on Smartphone's and many products are accessible for free or at reasonable prices. We systematically analyze the security implications of the capability to load malicious dynamic code in Android apps. We assess an Android Antimalware software tool to identify try to load malicious code and from the study of many online applications we observed, that malicious code is loaded in an insecure way is a major issue. We also show how malware can use code-loading techniques to avoid detection by develop a theoretical weak point in current Android malware protection.

III. Figure.

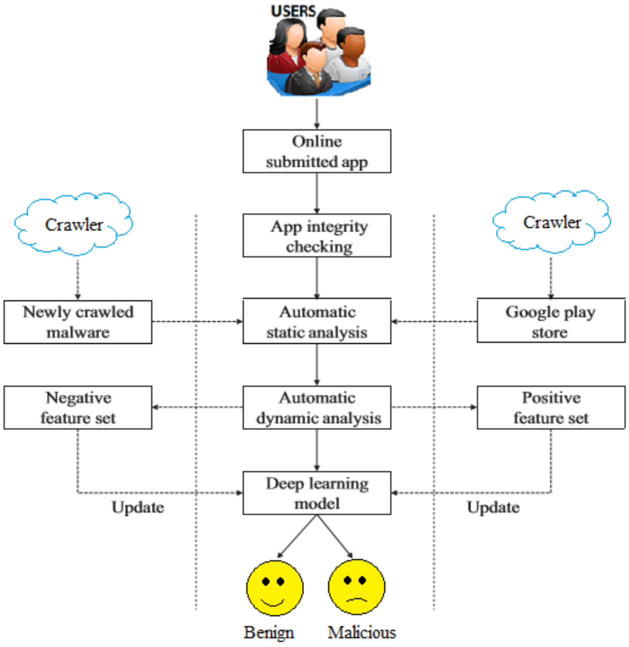

Fig. Framework of DroidDetector.

The ability of the deep learning model to detect Android malware and make an in-depth analysis on the features that deep learning essentially exploits to characterize malware, we conducted experiments on three public app sets. One benign app set was randomly crawled from the Google Play Store, which contains a large-scale apps. Although there might be a few malicious apps hidden among them, we regard all of them as benign apps. Another two malicious app sets were respectively collected from the Contagio Community and Genome Project. So, the total number of malicious apps is benign apps.

IV. Conclusion

Deep learning is a new area of machine learning study. In this study, we extracted a total of 192 features from both static and dynamic analyses of Android apps and characterized malware using a DBN-based deep learning model. We designed DroidDetector and evaluated it with 20000 benign apps crawled from the Google Play Store and 1760 malwares collected from the well-known Contagio Community and Genome Project. The results show that using DroidDetector with a deep learning model can achieve a superior accuracy under different conditions, significantly outperforming traditional machine learning techniques. At present, DroidDetector has been deployed online for user testing. Moreover, we delved deeper into the features that deep learning exploits to characterize Android malware using association rule mining techniques. The evaluation of ten popular anti-virus softwares indicates that it is a matter of urgency to make changes in Android malware detection.

Acknowledgements

It is my immense pleasure to work on this project **Malware Detection in Android App Using Static and Dynamic Analysis**. I would like to thank Dr. Arunkumar Dwivedi, Principal, LoGMIEER College of Engineering for giving me such an opportunity to develop practical knowledge about subject. I am also thankful to Prof K. V. Ugale, Head of Computer Engineering Department for his valuable encouragement at every phase of my seminar work and completion.

References

[1] S. Poeplau, Y. Fratantonio, A. Bianchi, C. Kruegel, and G. Vigna, Execute this! Analyzing unsafe and malicious dynamic code loading in Android applications, in Proceedings of the 21th Annual Symposium on Network and Distributed System Security (NDSS), 2014.

[2] Y. Zhou and X. Jiang, Dissecting Android malware: Characterization and evolution, in Proceedings of the 33rd IEEE Symposium on Security and Privacy (Oakland), 2012, pp. 95–109.

[3] D. Barrera, H. G. Kayacik, P. C. van Oorschot, and A. Somayaji, A methodology for empirical analysis of permission-based security models and its application to Android, in Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS), 2010, pp. 73–84.

[4] Y. Aafer, W. Du, and H. Yin, Droidapiminer: Mining apilevel features for robust malware detection in Android, in Proceedinds of the 9th International Conference on Security and Privacy in Communication Networks (SecureComm), 2013, pp. 86–103.

[5] D. Arp, M. Spreitzenbarth, M. Hbner, H. Gascon, K. Rieck, and C. Siemens, Drebin: Effective and explainable detection of Android malware in your pocket, in Proceedings of the 21th Annual Symposium on Network and Distributed System Security (NDSS), 2014.

[6] M. Zhang, Y. Duan, H. Yin, and Z. Zhao, Semantics-aware Android malware classification using weighted contextual api dependency graphs, in Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS), 2014, pp. 1105–1116.

[7] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, Crowdroid: Behavior-based malware detection system for Android, in Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2011, pp. 15–26.

[8] Y. Bengio, Learning deep architectures for ai, Foundations and Trends in Machine Learning, vol. 2, no. 1, pp. 1–127, 2009.

[9] Z. Yuan, Y. Lu, Z. Wang, and Y. Xue, Droid-sec: Deep learning in Android malware detection, in Proceedings of the 2014 ACM Conference on Special Interest GroupData Communication (SIGCOMM, poster), 2014, pp. 371– 372.

[10] DroidDetector: A deep learning based Android malware detection engine, http://analysis.droid-sec.com, 2015.

[11] Contagio mobile malware dump, http://contagiodump. blogspot.com, 2015.

1. *smartphone platforms, Computers & Security, vol. 34, pp. 47–66, 2013.*