Malware Detection in Android App Using Static and Dynamic Analysis

R.H.Sonawane[1], P.K.Tate[2], S.A.Shinde[3], R.S.Bhole[4]
Student of Computer Engineering
[1234]Loknete Gopinathji Munde Institude of Engineering Education and Reseach, Nashik, 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.

Key Words: Android security; malware detection; characterization; deep learning; association rules mining.

1. 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.

2. COMPARATIVE STUDY:

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.

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.

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.

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.

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.

3. COMPARATIVE STUDY TABLE:

Paper Parameter	Paper [1]	Paper [2]	Paper [3]	Paper [4]	Paper [5]	Paper [6]	Paper [7]	Paper [8]	Paper [9]	Paper [10]
Paper Name	DroidMiner: Automated Mining and Characterization of Fine-grained Malicious Behaviors in Android	DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket	Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis	Android Malware Detection Using Machine Learning Approch	A Study of Android Malware Detection Techniques and Machine Learning	A Machine Learning Approach to Android Malware Detection	Malware Detection Techniques in Android	An Assess Android Antimalware that Detects Malicious Dynamic code in apps.	Detecting Malicious Apps in Official and Alternative Android Markets	HADM: Hybrid Analysis for Detection of Malware

	Applications									
Author	Chao Yang,Philip Porras.	Daniel Arp, Hugo Gascon	Guodong Zhao, Lei Xu	Prof. Ganesh Bandal. Hemant Chavan, Amol Shivpure.	Balaji Baskaran and Anca Ralescu	Justin Sahs and Latifur Khan	Pallavi Kaushik, Amit Jain	Miss. Srushti Hatwar1, Prof. Chetan Shelke	Yajin Zhou, Zhi Wang, Wu Zhou, Xuxian Jiang	Lifan Xu Dongping Zhang Nuwan Jayasena John Cavazos
Domain Name	Mobile Security, Android Malware Analysis and Detection.	Mobile Security, Android Malware Analysis and Detection.	PT, malware infections , DNS, intrusion detection.	Android Security, Android System, Permission Detection.	Android malware, smartphone security	Computer Security, Data Mining, Support Vector Machines	Android, Dynamic Analysis, Machine learning, Malware, Malware detection, Static Analysis.	Antimalware, malicious code, malware, Android, Smartphone	Mobile Security, Android Malware Analysis and Detection.	Computer Security, Data Mining, Support Vector Machines
Algorithm	1.DroidMiner's 2.Modality Generation	1. Self Organizing Map (SOM)	1.domain generation algorithm (DGA) 2.J48 decision tree algorithm.	1. J48 (OR) C4.5 2. NAÏVE BAYES	1. ML algo-rithms. 2.J48 decision tree and 3.Random Forest algorithms.	Weisfeiler-Lehman relabelling, machine learning algorithms	1.Leonid Batyuk et. 2. Sanz et 3. Enck et 4.clustering algorithm	1. K-Means 2.Support Vector Machine (SVM)	1. clustering algorithm	1.Shortest Path Graph Kernel (SPGK) 2.Floyd-Washall 3.Support Vector Machine (SVM) 4.MKL algorithm.
Plat-form	Android	Android	Android	Android	Android	Android	Android	Android	Android	Android
Techniques	1.machine learning techniques. 2.common code extraction techniques	1.machine learning techniques. 2.lineartime analysis and learning techniques	1.domain flux technique. 2.malicious DNS analysis techniques.	1.repackaging, 2.update attack, 3. drive-by download.	1.code obfuscation technique. 2.static and dynamic techniques. 3.machine learning techniques	1.metamorphic techniques	1.static and dynamic techniques	1.code-loading techniques	1.DroidRanger.	1.dynamic analysis techniques. 2.static analysis, dynamic analysis, and hybrid techniques.
Attacks	1.confused deputy attacks. 2. collusion attacks	mimicry and poisoning attacks	1.APT attacks 2.DDoS attacks	Update Attack	update attack	DDoS attacks	Update Attack	Code injection attacks	1. confused deputy attacks. 2. drive-by download attacks.	security attacks.
Issues	security issues	security issues	security issues	security issues	security issues	security issues	security issues	security issues, protection issues	security issues	security issues
Applications	Android and Facebook applications.	malicious applications from Android markets	malicious applications from Android markets	smartphone applications,security application.	malicious android appli-cations.	Android applications	Android applications	Android applications	smartphone applications	malicious applications from Android markets

Conclusion	DroidMiner is a new static analysis system that automatically mines malicious parasitic Code segments from a corpus of malicious mobile applications, and then detects the presence of these code segments within other, previously unlabeled, mobile apps.	DREBIN combines concepts from static analysis and machine learning, which enables it to better keep pace with malware development. Our evaluation demonstrates the potential of this approach, where DREBIN outperforms related approaches and identifies malicious applications with few false alarms.	We propose a novel system IDnS placed at the network egress points to detect malware infections inside the network combined with DNS traffic analysis.	We had survey on framework for classifying Android applications whether they are malware or normal applications. To generate the models, we have extracted several permission features from several downloaded applications from android markets.	A method that could lead to potential counteracting the update attack is discussed. The unavailability of a larger android malware dataset remains a great problem in evaluating various ap-proaches. With a proper dataset shared among researchers, a system that learns a new malware and share that knowledge to all the mobile devices, so that they can protect themselves from future attacks, could be developed.	We tested our system against a collection of 2081 benign and 91 malicious Android applications. For each datapoint, we selected a random subset of the training (benign) applications and performed k-fold cross validation. In addition to the full kernel, we also trained against each individual kernel separately.	This model which combine features of both static analysis and dynamic analysis and machine learning algorithm. All these techniques are combined so to obtain maximum accuracy in detecting malicious samples.	Our analysis shows that the ability of Android apps to load additional code at runtime causes major security issues. We were able to show that an astonishingly large portion of existing applications is vulnerable to code injection due to download and access apps from unofficial sits	Permission-based behavioral footprinting and heuristics-based filtering. We have implemented both schemes in DroidRanger and the evaluation results of successfully detecting 211 malicious apps and uncovering two zero-day malware in both official and unofficial marketplaces demonstrate the feasibility and effectiveness of our approach.	we propose a hybrid Android malware classification method named HADM. We first evaluate the per-formance of 16 feature vector sets and 4 graph sets generated from 10 static and dynamic features collected from Android applications.

4. 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.

ACKNOWLEDGMENT:

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. Y. Zhou, Q. Zhang, S. Zou, and X. Jiang. Riskranker: scalable and accurate zero-day android malware detection. In Proc. of the 10th MobiSys, 2012.
2. A. Reina, A. Fattori, and L. Cavallaro. A system call-centric analysis and stimulation technique to automatically reconstruct android malware behaviors. In Proc. of European Workshop on System Security (EUROSEC),April 2013.
3. Wen Liu. Mutiple classifier system based android malware detection. In Machine Learning and Cybernetics (ICMLC), 2013 International Conference on, volume 01, pages 57–62, July 2013. doi: 10.1109/ICMLC.2013.6890444.
4. Mark A. Davenport, Richard G. Baraniuk, and Clayton D. Scott. Tuning support vector machines for minimax and neyman-pearson classification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(10), 2010.
5. S. Zhao, X. Li, G. Xu, L. Zhang, and Z. Feng, “Attack tree based android malware detection with hybrid analysis,” in Proceedings of the IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2014.
6. L. Xie, X. Zhang, J.-P. Seifert, and S. Zhu. pBMDS: A Behavior-based Malware Detection System for Cellphone Devices. In Proceedings of the 3rd ACM conference on Wireless Network Security, WiSec ’10, 2010.
7. S. Zhao, X. Li, G. Xu, L. Zhang, and Z. Feng, “Attack tree based android malware detection with hybrid analysis,” in Proceedings of the IEEE 13th International Conference on Trust, Security and
8. Privacy in Computing and Communications (TrustCom), 2014.
9. L. Xie, X. Zhang, J.-P. Seifert, and S. Zhu. pBMDS: A Behavior-based Malware Detection System for Cellphone Devices. In Proceedings of the 3rd ACM conference on Wireless Network Security, WiSec ’10, 2010.
10. S. Zhao, X. Li, G. Xu, L. Zhang, and Z. Feng, “Attack tree based android malware detection with hybrid analysis,” in Proceedings of the IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2014.
11. A. Mylonas, A. Kastania, and D. Gritzalis, Delegate the smartphone user? Security awareness in smartphone platforms, Computers & Security, vol. 34, pp. 47–66, 2013