International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

ANDROID MALWARE DETECTION

Margert Sharmila F
Associate Professor, Dept. of Computer Science and Business Systems
SKCET, Coimbatore, India

Jaisakthi K
Dept. of Computer Science and Business Systems
SKCET, Coimbatore, India

Pooja R
Dept. of Computer Science and Business Systems
SKCET, Coimbatore, India

Arshad Mohaidin A
Dept. of Computer Science and Business Systems
SKCET, Coimbatore, India

Abstract:

Now-a-days we could see the most of android mobile phone users, bringing android operating system into the market also increases the impact of mobile operation system malware . Althought we have many anti-malware software to build a protective wall against malicious software that is not very effective solution. Here we learnt about many malicious software and its way of affectiong the android operationg systems to break the security walls and to mis-use an individual personal information. We are about to provide a deep learning based software solution to find whether an android operating system based mobile phone is affected by malware not in the safe state.

Keywords

Android Security, Malware Detection Technique, Deep Learning based Malware Detection

1 Introduction:

In our daily routine mobile phones plays a hude role in it. We use mobile phones for all the activites we do today, as it provides comfortness to our lives. Application in miobile add the reason to use at all times. Lifestyle in current times has improved a lot due to mobile phone applications. Mobile devices have various detecting sensors and indicators in it, like global positioning sensor, sound detection sensor and also many useful sensors. As the saying goes ‘Every coin has two sides’, Though mobile phone application is developed under the motive to help people it also has its own risk.

Therefore we are in need of any new technology that stops the application users from facing the risk of malicious appplications and being a jokers to the technical threat. The operating system that has more physical strength is Android, so it also serves lot of risk.

The current solution we have for malicious application detection in andriod operating system is not ask plently of Question and permission request before installing any appplications. But if the user is

not completely aware of the application he must face its consequences. To know whereter an appplication is malacious or not the user of the android mobile must have complete knowledge about the application.

By asking the same set of question for both malicious application and secured appplication the user must have a mindset to skip all the question and only focus on installling the application , this method only increases the threat of the android mobile users.

The Android operating sytstem has its own protection wall, Though a malware is installed in the android mobile, after successful installation the user has the opportunity to decide the permission to be given to the respective application.

Alll these above mentioned security system are present in the android system, but there still exust the threat of malware in every nook and corner of the appplication being used, the user may not know we have a mallicious application in our android mobile phone and using it in an unsafe way, then he must face the consequence.

2 Literature Survey:

1. MalDozer:

Android system is enjoying its success peroid over last few decades.

As it gorws it is not only avaliable in the mobile operating sytem fieldd but alse step its foot in the field of Internet of Things. This is good at one side, but on the other hand , it is one of the tasty prey fot the malicious appplications. Hence, this currrent environment is need of software that detects malicious application and block its installation process from android devices. Here we came up with MalDozer a self detion system for detecting malware application in android operating systems. MalDozer is a deep learning based malware detection software that helps to identify malicious appplications and hepls to stay away from it.

MalDozer teaches itsely using the API function calls of malicious and secured application of real world example to detect the malware application at the future times.

2. Detection of Droid:

Android operating system is enjoying its succcess times during last few decades, so everyone has an eye on it and wants to break its security walls, some attempts to break such security walls fails and some not . One such succcessful atttempt is malware. Behind every secured appplication there is some type of malware associated to it. In order to elimate only the malicious part of each application android, Andoid is trying its best possible ways. The android organization is need of a trained deep learning based framework that detects the malicious appplication and provide the suppport to the security wall that had previously build by the android operating system.

3. Deep Learning Droid:

Malicious appplication are mainly used by people with some il-legal intensions to make money from it, they mis-use the personal and sensitive information from users mobile and tries to gain financial benefit from the application users. Although technology has grown a lot, thses kind of incidents are often happpening.

To avoid this situation android has tried many solutions to detect the malicious application and stops its execution even went on application ban. But malware has been developing from time to time, so detection technique becomes inefficient to detect the malware. Growth in detection technique is

comparatively slower than the evolution of malicious application. So it becomes harder to detect those application.

4. Flow in the Deep Learning:

Android wants to provide Flexiblity to both developers and the operating system users. By doing so, the rate of malicious application affecting android has gone to top. But later on, android found its fault and wants to rectify it, that leads to the raise of security questions and permission related questions in the android devices.But the out dated security checks like patterns, detecting abnormal mannersim of individual are insufficient to deat with novel malicious application. To address this strugggle deep learning based framework is found to classify appplication as malicious or safe.

5.Learning Malware Feature and Detection

The evolution and technical development of malicious virus has reduced the protecting power of android operating system, thus creates the threat among the android users.Users losee the confidence in android devices. We are planning to use a to use a deep-learning based frameworkto solve this scenerio.For that we are trying to get the five types of features throght static analysis of opertaing system. After that the functionality of appplication can be learnt throgh deep-learning process.

6. Malware Detection using API:

Due to the trememdous development in android system, the malicious appplication afffecting it has also became stronger than before, due to this malware detection has a strong place in cyber security. In the currrent society the maximum level of protection in android against malware is the signature-based approach and asking permission related questions. Due to the evolution of malware it is no longer efficient. This case increases the need for deep-learning based framework that detects the malware without installation. Here we are evaluating the API method calls of various applications and detects the appplication is malicious or safe. Deep Learning framework can train itself, they have the ability to learn on their own. We generate classification codes from API, after these classification code generation, we will move on the categorize application.

7. SURVEY - MALWARE DETECTION IN ANDROID:

The count of people using android devices has grown a lot in the past few decades. The risk in android system has also grown. As, the attackers wants to break the android protection, the risk of using android devices is musc more now. Android users have access to installl plenty of application and software from android play store. Sowetimes the appplication in the play store may contain malware, which leads the attackers to access users personal and sensitive data. Application in the queue to be lanunched in the play store usually undergoes a several level of testing and checking. However crawl application are tested and then generated a tesr and check result.crawl appplication include type, tap and swipe. Though all the level of checking is done before launching an application in app store, some malware is capable of tresspass the check levels and has the ability to successful get launched in the app store.

8. Security in Android Devices:

Mobile Mobile phones had became the unavoidable device in the current world, As it has help install seveeral appplication in it and Helps to play intesesting games, act as travel guide by providing route and location, hepls us to send the message via e-mail, chat ans sms facilities.The API's of the android application had made android operating system as popular and open source system among the developers. Due to the tremendous growth of malware, the attackers urges to bring the drag the android market down, thus let them to create malicious application and attack the android users by mis-using the personal ams sensitive information. By doing so, the are capable of breaking the andrid system's protection wall.

3 Problem statement:

Android has a security check process, where the application waiting in the queue get launched undergoes scanning for some period of time, but the application does not exhibit its malicious tendency at rthe scanning time and gets launched. Android store also checks during an installlation of appplication at the initial code, so the malicious cannot be detected at that stage and tresspasses it.
The same level of checking is done for all the kind of apppliactionm so malicious application canot be detected though this type of check.
The deep learning based frameworkto auto detect malicious application without the requirement of instllation process is MalDozer, it has the ability to train itself to diffrentiate between malware and safe appplication from the API function calls.

5 Results and Discussion:

The architecure of MalDozer has passed several complx test and able to detect the malicious application usuing the deep learning framework. MalDozer indenfies the type of application using a signle neron at the result end ang gives it result. There are difffrent neoron takes place in the MalDozer test each neuron represents only a single type of malware.

One deep learning-based Android malware detection method is Droid Deep. The method used here is a DBN-based deep learning model for malware detection. Droid Deep needs a single application demo to help define traditional indicators of malware action. Droid Deep has a substantial set of fixed analytics that extract its feature set from various sources such as API calls and Manifest.xml files. Droid Deep aims to differentiate apps into different types such as requested permissions, used permissions, sensitive API calls, actions, and app components.

This static analysis-based feature extraction method requires an Android app .apk file. After extracting the .apk file using apktool and Droid Deep, the main focus is to properly parse the two files like AndroidManifest.xml and classes.dex. The above functions are extracted by using these two files. For feature extraction the tools and parsers are used by Droid Deep.

8 Conclusion:

In this document, we have explored different types of Android malware detection techniques by the use of different deep learning techniques. Due to Android's open nature, a myriad of malware is hidden in dozens of harmless apps on the Android market. This malware can be a crucial danger to Android security. An attacker get to view user information as below:

Messages, contacts, bank his mTAN, location, etc.Here we explore various Android malware detection techniques, including:MalDozer, Droid Detector, Droid Deep Learner, Deep Flow. MalDozer uses convolutional neural networks to detect malware. It uses static analysis methods and API method calls as a feature to detect if an application is infected with malware.

Droid Detector inspires Deep Belief Network for detection. They use static and dynamic analysis with features such as:

Permissions, APIs, and dynamic behavior for malware detection. The Droid deep learner method also uses the Deep Belief Network for malware detection.

---

9 References:

[1] E. B. Karbab, M. Debbabi, A. Derhab, and D. Mouheb, “MalDozer:
Automatic framework for android malware detection using deep learning,” Digital Investigation, vol. 24, 2018.

[2] Z. Yuan, Y. Lu, and Y. Xue,
“Droiddetector: android malware characterization and detection using deep learning,” Tsinghua Science and Technology,
vol. 21,
no. 1, pp. 114–123,
2016.

[3] Z. Wang, J. Cai, S. Cheng, and W. Li,
“DroidDeepLearner: Identifying Android malware using deep learning,”
2016
IEEE 37th Sarnoff Symposium, 2016.

[4] D. Zhu, H. Jin, Y. Yang, D. Wu, and W. Chen,
“DeepFlow: Deep learning-based malware detection by mining Android application for abnormal usage of sensitive data,”
2017 IEEE Symposium on Computers and Communications (ISCC),
2017.

[5] X. Su, D. Zhang, W. Li, and K. Zhao,
“A Deep Learning Approach to Android Malware Feature Learning and Detection,” 2016
IEEE Trustcom/BigDataSE/ISPA, 2016.

[6] S. Hou, A. Saas, Y. Ye, and L. Chen,
“DroidDelver: An Android Malware Detection System Using Deep Belief Network Based on API Call Blocks,” Web-Age Information Management Lecture Notes in Computer Science,
pp. 54–66, 2016.

[7] R. Zachariah, K. Akash, M. S. Yousef, and A. M. Chacko,
“Android malware detection a survey,”
2017 IEEE International Conference on Circuits and Systems (ICCS), 2017.

[8] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, and M. Rajarajan,
“Android Security: A Survey of Issues, Malware Penetration, and Defenses,” IEEE Communications Surveys & Tutorials,
vol. 17,

no. 2, pp. 998–1022,
2015.

[9] A. I. A'Fifah, A. Ritahani, and A. Ahmad, "Comparative Performance of Deep Learning and Machine Learning Algorithms on Imbalanced Handwritten Data," International Journal of Advanced Computer Science and Applications,
vol. 9,
no. 2,
2018.

[10] V. Rao, K. Hande,
"A comparative study of static, dynamic and hybrid analysis techniques for android malware detection," International Journal of Engineering Development and Research,
pp. 1433-1436,
2017.https://doi.org/10.1016/j.jhlste.2022.100399.

[11] A. Kapratwar, F. D. Troia, and M. Stamp,
"Static and Dynamic Analysis of Android Malware,"
Proceedings of the 3rd International Conference on Information Systems Security and Privacy,
2017.

[12] K. Sugunan, T. G. Kumar, and K. A. Dhanya,
"Static and Dynamic Analysis for Android Malware Detection,"
Advances in Intelligent Systems and Computing Advances in Big Data and Cloud Computing,
pp. 147–155,
2018.