A Survey: Android Thread & Spamming Detection Approach Analysis

Priyanka Usrate*, Prof. Damodar Tiwari** and Dr. N. K. Tiwari***
*(0112CS15MT12), *-***Bansal Institute of Science and Technology, Bhopal

Abstract: Android device and various applications are useful paradigm today in every sector and group of people. Different attack and scenarios are generating towards security and threats. Different study on creating an efficient framework for designing and analyzing the android structure and multiple threads detection study is performed. An analysis study on virus, malwares and threads is performed by several research groups. In this paper study of different malware detection analysis, detection technique over the framework, installation API & their component is studied. In recent Paper author has given MADAM approach for malware detection in Android system and architecture, where they investigated study of incoming application installation, running application behavior learning. Further the Blocking of application according to their usability and activity on the device structure components. Further a survey is studied from various intrusion detection technique which deals with the detection of anomaly and their prevention structure, as well as their pros and cons of using it.

Keywords: Mobile Computing, Malware, malware detection, Mobile architecture, Android antivirus.

Introduction

From security point of view, the increasing demand of network connectivity makes the system insecure. So we need a complement that can cope / prevent the security breaches in system. Unfortunately, in many environments, it may not be feasible to render the computer system immune to all type of intrusions. The motivation behind this project is to develop a complement system i.e. Intrusion detection system (IDS) that can prevent all possible breaks-ins. Generally, Intrusion detection system (IDS) has three component that is detection component, investigating component, and post-mortem component. The detection component identifies security breaches. The investigation component determines exactly what happened, based on data from the detection component. This component may also include the gathering of further data in order to identify the security violator. Finally, the post-mortem component analyzes how to prevent similar intrusions in the future. With the emergence and the proven utility of the intrusion detection concept, the detection component is beginning to receive more attention. There are many approaches to find intrusions under detection component. Since volume of data dealing with network is so large, this collection concentrates heavily on the use of data mining in the area of intrusion detection. Classification is one of the effective techniques under data mining that can be used for intrusion detection. Two common knowledge representations for classification technique are IF-THEN rules and Decision tree.

The classification is required in order to find intrusion detection by the algorithms which help to separate the outlier using the technique. Thus in this research we are working on classification for IDS application using different approach already been discussed in different literature.

Mobile computing is a recent technological development in the computing field in which mainly focused on designing of services which can be provided to the users in same way as the basic utilities like food, water, gas, electricity and telephony. In this technology services are developed and hosted on the Mobile (a network designed for storing data called datacenter) and then these services are offered to users always whenever they want to use. The Mobile hosted services are delivered to users in pay-per-use, multi-tenancy, scalability, self-operability, on-demand and cost effective manner. Mobile computing is become popular because of above mention services offered to users. All the services offered by servers to users are provided by Mobile service provider (CSP) which is working same as the ISP (Internet service provider) in the internet computing. In the internet technology some innovative development in virtualization and distributed computing and accessing of high speed network with low cost attract focus of users toward this technology. This technology is designed with the new concept of services provisioning to users without purchasing of these services and stored on their local memory.

Malware is the combination of two words called malicious and software, thus malwares are the software which puts malicious and harmful effect on the software, operating system or other components. A survey over various malwares and malware detection techniques [13] is presented which provides a description of the various types of attacks and classes of malwares, like network based malware attacks, ordinary malware attacks etc. in network malware, malwares like spywares are used to put harmful effect over users machine, in ordinary malware malwares like autorun.inf system.inf etc. are used to put harmful effect over users machine. There are various techniques presents by the user to detect malwares in the system. Like in [8] a hybrid signature call graph scheme is used to provide a malware detection for the various types of malware

attacks, in [11] a semantic aware malware detection technique is presented which uses the semantics of the files to detect malware. In [9] metamorphic malware detection technique to detect various type of malwares is presented. In [10] a file content and relation of these files is used to provide a malware detection the Mobile computing which provides a secure mechanism to transfer data in Mobile. In [12] a flow for the malware detection technique is presented, and security mechanism for the [7] which takes a multi agents architecture to provide security for the various type of data is presented.
Further this paper organizes as follows
II Literature Review, in this section a description over the various malware detection techniques is presented. III Conclusion.

Literature Review

A review over the various techniques which used for malware detection in Mobile computing is presented in this section.
In [1] an algorithm and architecture for detection of anomaly and malware in android mobile is presented. This paper presents MADAM, which is Host based architecture and malware detection platform. A multilevel and behavior based algorithm approach is followed by the author. Behavior based pattern detection architecture was used by this technique. This architecture work on detection for Rootkit, SMS Trojan, Spyware, Botnet, Ransom ware , installer , Trojan as intrusion entity. A different level of detection such as application installer and kernel level, further the activity running level and other given user activity level finding of malware is presented in this paper by authors. They have done all type of global and activity monitoring in their execution. The presentation of experiment was performed with android application build and execution. Where the total 2,800 application in different 125 categories is taken for testing. Finally they have shown the detection of different virus and attacks on mobile and shows the efficiency and detection rate in their system while compare to other existing mobile scenario. They have performed rooting and overhead is proper according to their given algorithm. A further working on the system with enhancement of limitation with increasing working with pattern detection and solving the problem of behavior based detection is left by the author.
In [2] MADAM architecture by the author of [1] is further performed with the pattern based extension and detection over the data. An early execution and detection over the android architecture and framework is performed by the authors. They have able to manage 10 real-time malware. FPR, detection rate, monitoring activity log in the mobile phone usage is also performed by the author. The classifiers are trained for the anomaly malware detection and thus an monitoring is performed by the authors. The further expected extension of the author was given as detecting behavior action and creating a database of behavior to perform effective monitoring. High level monitoring, triggering alarm to the user on another mobile is left in their future work.
In [3] A technique of malware detection approach using its traffic analysis feature. According to them a new work on the basis of traffic based efficiency and malware monitoring is performed by them. They have analyze the traffic feature, found the differentiate in between the features provided. Further the build automated classifier performed the anomaly malware classification. The category of their malware bots are AnserverBot, Bgserv, DroidDream etc., they leads to main core area of working anomaly malware as root. A traffic analysis of packet such as TCP and UDP is given as monitoring, thus a packet and filtration detection is performed by the author. Android emulator, remote server monitoring, command information.
In [4] A technique which is working on matric basis is performed by the author. Permission and its usage model for any of the application, malware filtration and execution is performed by the author. A filtering process for suspicion entity and data is derived in this paper. A complete permission based filtration technique is opted by the computer. They have developed the code in matlab for their algorithm and proven the efficiency of their algorithm. But still the real time implementation is not been performed and which is left for the future work. They have worked on static dataset of permission and application dataset of 122 apps. 71331 number of permission is being used by the system to perform the algorithm.
In [1] a malware detection technique to detect malware and rootkit is presented. That Takes a system call monitoring and system call hashing together and a support vector machine based external host monitoring system is also used. In monitoring system call all the system calls triggered by the users, are monitored over the parameter before execution. In system call hashing, all the stored monitored system called copies are checked before installation. Then a support vector machine based system is used which classify all the malware and rootkit attacks in virtualize Mobile system. But that technique suffers in accuracy thus a new technique to provide accurate results for intrusion detection.
In [2] a support vector machine based technique is presented to detect intrusion in the Mobile computing architecture. In this a support vector machine based monitoring system is used at hypervisor level to detect malware in Mobile computing system. In Mobile virtualization there is various type of threats can be found which requires an enhanced functionality to deal with such Mobile computing threats. Thus an enhanced mechanism is required to provide an accurate result for this problem.
In [3] a description over the various malware detection techniques which used for the intrusion detection is presented. In that various machine learning techniques can be used to provide a detection mechanism for Mobile computing. In that way it requires an enhanced technique to pride accurate intrusion detection for such techniques.
In [4] a malware detection technique for virtualize Mobile environment is presented. There are various system resilience related risks are occurred in these virtualizations techniques. New technique is required which can deal with the issues related to the risk in the programming. In that technique a NAE (Network Analysis engine) and system analysis engine is

used to deal with such issues. But these techniques are not efficient to deal with such issues new technique is required to provide an enhanced performance for malware detection.

In [5] a new malware detection software technique is presented, which provides an enhanced functionality for detections of malware and enhanced forensics capability and improved deployability for the various software. But that technique this technique is still require an improvement in malware detection to provide an enhanced functionality for the better intrusion detection is required.

In [6] a review over the various malware detection techniques is presented, which provides a brief overview over the malware detection and malware detection techniques. There are various techniques like host based technique, malware detection in virtualized Mobile scenario; malware detection for guest user is generally used to provide a malware detection system.

In [7] author worked on a model which is software defined networking based model performed in Open modeler with Apache Java functionality is performed. A testbed setup with i7 system and 8 GB RAM is considered for the implementation. A topology for the different component, their communication setup. Floodlight controller based system for controlling the architecture structure is driven performed in their proposed work. Suspicious network malware detection with real time traffic data analysis is performed by them. An learning of malware and its characteristics activity is performed by the future work is stated by the author.

In [8] an ontology based malware detection technique for the Mobile data is presented. Malwares are the combination of malicious and software which means a harmful software. Thus definition for the various malware, is presented. In that a K-mean clustering technique is used to classify various malware attacks into different classes. On the basis of these classes a malware detection to detect malicious software is performed. In Mobile user uses internet to access various applications, which can be induce any malicious software into user's machine. Thus a malware detection using these definition is performed to detect threats in that application.

Proposed Work

As per the previous work and their limitation is monitored by the work functioned by us . here a conclusion is got that the further extension can be done in following area of learning.

1. Auto-Learning process of the data and malware features need to be performed which can be further be done by efficient ANN technique such as KNN technique.
2. An security option can be opt while performing the network based analysis and real-time analysis detection over the algorithm.
3. An auto-learning, enhanced security based model is further going to derive by us with network usage analysis in the proposed system.

Conclusion

In current scenario there are various technique are used for intrusion detection in Mobile computing. There are various on-demand services are provided to the user, these techniques requires an enhanced functionality to deal with such issues. A brief description over the techniques which used for malware detection in Mobile computing is presented in this paper. There are techniques like n-gram based pattern detection, IDS signature, malware detection in virtualization etc are used. An enhanced technique for the future work is proposed to provide better malware detection in Mobile computing scenario.

References

[1] Andrea Saracino, Daniele Sgandurra, Gianluca Dini and Fabio Martinelli," MADAM: Effective and Efficient Behavior-based Android Malware Detection and Prevention", IEEE 2015.

[2] Gianluca Dini , Fabio Martinelli , Andrea Saracino , and Daniele Sgandurra, "MADAM: a Multi-Level Anomaly Detector for Android Malware", Springer 2015.

[3] Anshul Arora, Shree Garg, Sateesh K Peddoju, "Malware Detection Using Network Traffic Analysis in Android Based Mobile Devices", 4 Eighth International Conference on Next Generation Mobile Applications, Services and Technologies 2014 IEEE.

[4] Mahmood Deypir," A New Approach for Effective Malware Detection in Android-based Devices", 13th International ISC Conference on Information Security and Cryptology (ISCISC2016) September 7-8, 2016; Shahid Beheshti University – Tehran, Iran.

[5] Gates, C. S., Chen, J., Li, N., & Proctor, R. W. (2014). Effective risk communication for android apps. Dependable and Secure Computing, IEEE Transactions on, 11(3), 252- 265.

[6] Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013, April). Privacy as part of the app decision-making process. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 3393-3402). ACM.

[7] Ruofan Jin, Bing Wang," Malware Detection for Mobile Devices Using Software-Defined Networking", 2013 Second GENI Research and Educational Experiment Workshop.

[8] Geneiatakis, D., Fovino, I. N., Kounelis, I., & Stirparo, P. (2015). A Permission verification approach for android mobile applications. Computers & Security, 49, 192-205

[9] Pallavi Kaushik, Amit Jain," Malware Detection Techniques in Android", International Journal of Computer Applications (0975 – 8887) Volume 122 – No.17, July 2015.