Advances in Computing 2017, 7(2): 19-22
DOI: 10.5923/j.ac.20170702.02

Behavioral Malware Detection for Bus Ticket Booking

Arpana L. Shetty*, Sunitha Guruprasad

Department of Computer Science and Engineering, St. Joseph Engineering College, Mangaluru, India

Abstract Malware is a program or a file which can gain entry to private system without the user's permission. Malicious users can attack the web data and perform malignant activities. It can also access the confidential data present in the system. This paper focuses on the case study of ticket booking system. The main challenge here is to find the malicious users and blacklist them. Malicious users can be detected based on the some system call behaviors such as name and email id. The behaviors are predefined, if current user activity matches with predefined activity then the particular user is considered as malicious and can be blacklisted. This will help the end user to get the available bus seats on time.

Keywords Malware, System Call, Seat Chart, Malignant Activity, Behaviors

1. Introduction

Malwares are programs or it can be any documents or files which can gain access to user's private system without their attention. Web data can be attacked by malicious users and perform Malignant Activity.

This paper focuses on the case study of bus ticket booking system. Usually ticket booking website contains seat chart which has available seats and unavailable seats. Sometimes two users may select same seat and pay for the same without knowing each other's actions. So in ticket booking website, there will be three states. When the user selects any seats, that particular seat will be blocked for some period of time which is known as blocked state. This blocked state changes to booked, if user does the payment within that particular period of time. That seat will be released if the payment is not done within that period of time, the state here is known as released state.

Sometimes, the seats will be blocked simply and not booked. This blocking may be done by some malicious private bus agencies. If they do so, users may think that all seats are full in this particular bus agency and they will search in other private bus agency services. These malicious bus agencies will select the seats randomly, so that seat will be blocked for some duration of time. But the payment for the seat will not be done. In this blocked period, that particular seat will be unavailable.

If any other user searches for that particular seat, it will be blocked. This may be mistakenly done by genuine users also. But the system may consider that users as malicious users. The problem is to find out malicious users and non - malicious users. Malicious users are detected based on the behaviors which are predefined.

IP address, name and email id etc are the behaviors which the system can consider. These behaviors can be distinguished into two sections. The sections are network based and system call based. System call based behaviors such as email id and name are considered. These behaviors have to be defined previously. If the predefined behaviors and user's activities match with one another, then that user can be blocked. This will help the bus users to get available seats on time.

The rest of the paper is coordinated as follows. Section II briefly explains an overview of the existing system and their related work. Section III provides detailed description of proposed methodology. Section IV represents the results. Finally, section V presents conclusion and the future scope.

2. Related Work

Different detection approaches have been introduced to detect the malwares. In [1] malware detection for android devices is done based on the behaviors. There are two approaches in this. First is based on network method. All the remote place's URLs are acquired by network analysis for which application is in touch. Later pattern matching will be done with respect to malicious domains which are familiar. Second is based on system calls. Frequencies are measured for system calls of all the applications. Then it is matched with respect to familiar malicious domains. Data mining methods are used for detection of malwares in [2]. API series are considered as malicious behaviors in this method. User's secret data will be captured by malignant applications. Kernel based behaviors are used for the analysis of android malwares in [3]. This method has log collector and log analyzer. System calls are recorded by log collector and filtering of events will be done using target applications. Log

* Corresponding author:
arpanashetty23@gmail.com (Arpana L. Shetty)
Published online at http://journal.sapub.org/ac

collector will reside in Linux layer. Log analysis application will match the actions with regular expression's signature to detect whether the activity is malicious or not. Paper [4] uses map reduce with system call analysis to detect malwares. Collection and analysis of system call is done in this method. System call analysis will increase the performance as well. Map reduce will analyze the system calls on servers and reduce client's performance. Paper [5] is about native malware detection methods. It is based on static analysis, selection of features and ensemble classifiers for smart phones which are android. Without the use of external server board smart phone analysis is done here. This method exactly classifies the applications.

3. Proposed System

Malware is a file or program which access to private system without user's acceptance. Web data can be attacked by malwares and secret data can be disclosed in public. Ticket booking system is taken as the case study for this project. The seat cancellation done three times or more than that by blocking is considered as malicious activity here. This work may be done by other bus seat booking agencies, sometimes mistakenly by genuine users. So the problem is to differentiate between malicious and non malicious users. The main challenge here is to find out the malicious users and to block them based on the predefined behaviors. So the end users can easily book the bus seats without any problem of blockage.

Steps of proposed method:

Step (1): System call based malware detection will be done which is based on the behaviors of malware. Name and email id are considered here as malware behaviors.

Step (2): If predefined behavior and current behaviors match with one another, then the current activity will be considered as malicious activity. If cancellation of seats is done more than two times from same name and email id, then this activity will be called as malicious activity.

Step (3): Finally malicious users has to be blacklisted. This will prevent the blocking of seats. The users will get the available bus seats without any problem of blockage.

Admin will be the owner of ticket booking website. Buses can be added by admin to the service station. Admin has the ability add buses to which service centre can provide bus services. Blocked users can be unblocked only by the admin. Admin will be having a special power of unblocking the malicious users after a particular time. Blacklisting of users will be done when his activity is considered as malicious activity. In this case, the users will be blocked if they cancel the seats more than two times from same name and email id. But the malicious users can be deleted from the blocked list by admin after some period of time. So that the user is now able to access the website since the user is unblocked. The particular user will become non malicious users after they are deleted from blocked list.

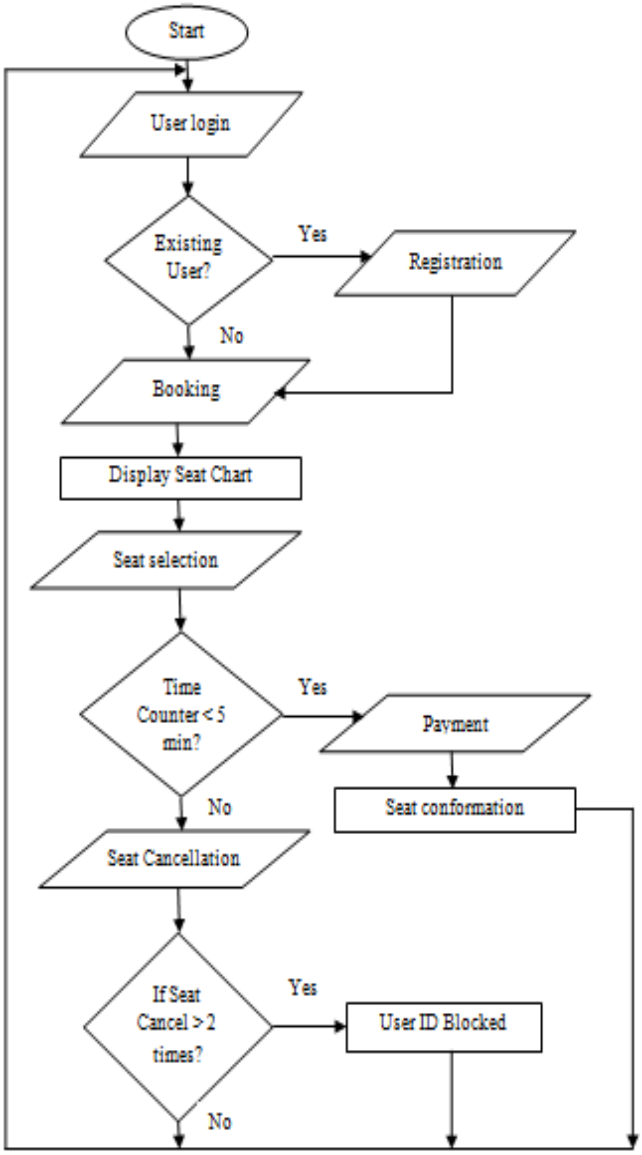

Figure 1. Flow Diagram

Initial page is the login page through which both admin and user can login to the system. Particular username and password has to be entered for admin to login. Once the admin is logged in they will be able to access two pages. First one is bus page through which admin can add buses of his choice. Next one is block page, where the admin can delete the blocked users from the list to make them non malicious users.

The new users will have to register and login using particular username and password. Registered users can directly login through their username and password. Once the user is logged in booking page can be accessed. The booking details have to be filled for the seat selection. When a seat is selected by user, timer will start for 5 minutes. Within those 5 minutes if the payment is done means seat will be booked, otherwise seat will be released. If the seat is cancelled more than two times from the same name and email id then the particular user will be blocked. Then the

particular user will be considered as malicious user as cancelling the seats more than two times is considered as malicious activity.

4. Results

User will be considered as malicious user and blacklisted when the seat is cancelled by him more than two times before the payment is done. Name and email id are considered as system call behaviors which is used for blocking. Once the user is blocked and cannot access the system since user will be considered as malicious user. User can only be able to access the system after admin deletes him from the blocked list.

Blocked list is a list of malicious users who are blacklisted. User will not be able to access the booking service after being blacklisted. Admin has the ability to unblock the blocked users from the list. Admin can delete the users from list, thus making him non-malicious. The ticket booking website can be accessed by user after the user is unblocked. Once the admin unblocks the user, user can register and access the website and its services.

5. Conclusions

This paper focuses on the detection of malwares for a case study of ticket booking website using system call based behaviors. The name and email ids are used as system call based behaviors. Proposed method focuses on detecting malicious users and blacklisting them based on behaviors. One who simply cancels seats two times or more than that will be considered as malicious users. This will be a problem for users to book particular seats because of blocking of seats. So the proposed approach helps the users to conveniently use the website to book bus seats.

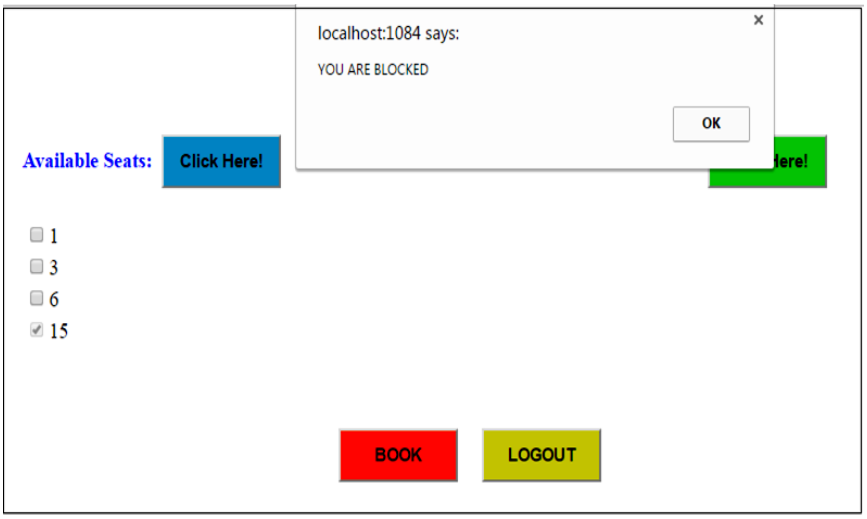

Figure 2. Seat Chart Page Blocking Condition

Figure 3. Blocked users list

Future Scopes

Time or location can also be used as system call based behaviors for malware detection. IP address can also be used as a network based approach to detect the malwares.

REFERENCES

[1] Mohammad Rakib Amin, Mehedee Zaman, Md. Shohrab Hossain and Mohammed Atiquzzaman, "Behavioral Malware Detection Approaches for Android", IEEE International Conference on Communications, DOI:10.1109/ICC.2016.7511573, Pages: 1-6, in 2016.

[2] Jiawei Zhu, Zhengang Wu, Zhi Guan and Zhong Chen, "API Sequences based Malware Detection for Android", in UIC-ATC-ScalCom-CBDCom-IoP, DOI:10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.135, Pages: 673-676, in 2015.

[3] Takamasa Isohara, Keisuke Takemori and Ayumu Kubota, "Kernel-based Behavior Analysis for Android Malware Detection", Seventh International Conference on Computational Intelligence and Security, DOI:10.1109/CIS.2011.226, Pages: 1011-1015, in 2011.

[4] Shun-Te Liu, Hui-ching Huang, Yi-Ming Chen, "A System Call Analysis Method with MapReduce for Malware Detection", IEEE 17th International Conference on Parallel and Distributed Systems, DOI:10.1109/ICPADS.2011.17, Pages: 631-637, in 2011.

[5] S. Morales-Ortega, P. J. Escamilla - Ambrosio, A. Rodriguez –Mota L. D. Coronado – De - Alba, "Native malware detection in smartphones with android OS using static analysis, feature selection and ensemble classifiers", 11th International Conference on Malicious and Unwanted Software, DOI: 10.1109/MALWARE.2016.7888731, Pages: 1-8, in 2016.

[6] Wei Peng, Feng Li, Xukai Zou and Jie Wu, "Behavioral Malware Detection in Delay Tolerant Networks", IEEE Transactions on Parallel and Distributed Systems, DOI: 10.1109/TPDS.2013.27, Pages: 53-63, in 2014.

[7] Dmitri Bekerman, Bracha Shapira, Lior Rokach and Ariel Bar, "Unknown malware detection using network traffic classification", IEEE Conference on Communications and Network Security, DOI: 10.1109/CNS.2015.7346821, pages:134-142, in 2015.

[8] Raymond Canzanese, Spiros Mancoridis, Moshe Kam, "System Call Based Detection of Malicious Processes", IEEE International Conference on Software Quality, Reliability and Security, DOI: 10.1109/QRS.2015.26, Pages: 119-124, in 2015.

[9] Chia-Mei Chen, Je-Ming Lin, Gu-Hsin Lai, "Detecting Mobile Application Malicious Behaviors Based on Data Flow of Source Code", International Conference on Trustworthy Systems and their Applications, DOI: 10.1109/TSA.2014.10, Pages:1-6, in 2014.

[10] Hsiu-Sen Chiang, Woei-Jiunn Tsaur, "Identifying Smartphone Malware Using Data Mining Technology", Proceedings of 20th International Conference on Computer Communications and Networks, DOI: 10.1109/ICCCN.2011.6005937, Pages: 1-6, in 2011.