RESEARCH ARTICLE OPEN ACCESS

Study on Detection of Internal attackers using Signature Detection Technique

P.Thamarai
Department of Computer Science and Engineering
Dr. M.G.R Educational & Research Institute, University, Chennai
Tamil Nadu - India

ABSTRACT
In today's modern world, a more number of user's authentication to the system is through a distinct user ID and password individually for each user, but this condition creates problematic situations when those user Id and password are acquired by an attacker. Signature Detection Technique method is used in this paper to prevent internal attacks and thus report it to the manager when it is made and also helps in tracking the source of the attack .This paper also contains the concepts of about how to maintain login profiles of each user, in order to find the attacker by comparing it with that of the original user habits. Further results are used as a general idea to implement new rules for intrusion detection systems. Thus, the internal attackers are not to be under estimated or to be taken the least care, as they are also the more important victims to be found. Since those victims can easily attack the system, if left without care in any of the organization internally.
Keywords:- Signature Detection Technique, Internal attackers

I. INTRODUCTION

Nowadays, computer systems usage has increased rapidly and well advanced. Owing to that, the systems can be misused by other users by following their attacking methods. Different methods of attacking the system such as eavesdropping attack, computer hacking, computer worm, and DoS (Denial of Service) attack is being used by the attacker. But in recent times, all those attacking methods have been improved and are tedious too. Security managers are unaware of the attack when those tricky attacking methods are done by an attacker. In this paper, data mining is employed, in which the data's about the employees in an organization are stored and retrieved for various purposes. In this modern world, threats related to attacking the system are increasing at a higher rate externally as well as internally. Internal Attackers in an organization has also got increased miserably, which becomes a tough task for the management to detect and find who the attacker is. So, this paper gives methodologies to find the victim who tries to attack the system internally. Moreover, this paper explains the concepts which could be highly useful in an organization. The concept of signature detection technique is used in this paper for the detection of internal attackers.

A. Data Mining

Data mining mining is the computational process of which discovers the patterns in large data sets . It is an interdisciplinary subfield of computer science. The overall goal of the data mining process is to extract information from a data set and transform it into an understandable structure for further usage. It is also the process in which patterns from the data is being extracted. Since many a number of data's are stored every year, data mining has become a more important tool to transform the data into information. . It is generally used in a wide range of profiling practices. They consists of involves four classes of the task ad arranges the data into predefined groups.

B. System Requirements

The following are the system requirements which are essential for this work.

1) Hardware Requirements: The Hardware components used are processors such as Pentium Iv 2.6 GHz, Intel Core 2 Duo, 512 MB DD RAM, 15" COLOR monitor, 40 GB hard disk. These are the hardware requirements which are essential for the study involved in this work.

2) Software Requirements: The Software tools used in this work are JSP, SERVLET, STRUTS, MYSQL, Windows, IDE, Net Beans, and Eclipse. These are the tools that are required in a system for the study on Internal Attackers.

II. MODULES

This paper has four modules each of which has its own characteristic features which follows a sequential order to get the result of study on the internal attackers by the usage of appropriate tools and mechanisms which are required for the study at a greater rate of accuracy and at a lower rate of redundancy, thus the various modules used in this work can be elaborated as follows:

A. User Interface Design
B. Control initialization
C. Mining User and Attacker Habits
D. Attacker Analysis and Graph model

A. User Interface Design

In this work, this module helps to design login window page .It focuses on the login design page with Partial knowledge information. If users want to access the application they need to login through the User Interface.GUI connects the user, Media Database and the login screen where user can input their user name, password and can access the application. In this module, swing package available in java to design the user interface. Swing is a widget toolkit for java which is a part of sun micro systems.

B. Control Initialization

In this module, Application Manager Interface Design plays an important role for the Manager to move login window to Manager welcome window. Manager will enter the salary details of users and allocate projects to the Team leader. System Framework is used for generating the user's habit file from which the attackers can be detected comparing the counts stored. The above algorithm is being employed in this module which is the most important in maintaining the user habit file which highly helps in the process of finding out the victim who tries to attack the system. Thus, this module stands as one of the important module of this work for detection of the victim. The following is the algorithm used in this module.

1)Algorithm: This algorithm which is used in this work is used to generate the habit file of the user, as the user habit file in this concept act as a pillar to find and detect the attacker who tries to attack the system internally. The Data sets used in this work uses the simple mathematical notations for the generation of the habit file. The mathematical operations used in this work are the simple arithmetic operations which in turn use the simple logics or ideologies for devising the habit file of the user using the system framework.

Algorithm 1: The algorithm for generating a user habit file
Input: u's log file where u is a user of the underlying system
Output: u's habit file

1. G = |log file| - |Sliding window| ;
   /* |Sliding windows|=|L-window|=|C-window| */
2. for (i=0 ; $i \leq G-1$; i++) {
3. for (j=i+1 ; $j \leq G$; j++) {
4. for (each of $\sum_{k=2}^{|\text{Sliding window}|}$(|Sliding window| − k + 1) k-grams in current L-window){
5. for (each of $\sum_{k'=2}^{|\text{Sliding window}|}$(|Sliding window| − k' + 1) k'-grams in C-window){
6. Compare the k-grams and k'-grams with the longest common subsequence algorithm;
7. if (the identified SC-pattern already exists in the habit file)
8. Increase the count of the SC-pattern by one;
9. else
10. Insert the SC-pattern into the habit file with count=1; }}}}

Fig.1 Algorithm used to generate a user habit file.

2) Data Sets: The data sets used in this module are as follows. Thus, these data sets are derived from the above algorithm, which is been used for the generation of the users habit file.

T_{total}

$$= \frac{(l-n+1)(l-n)}{2} \times \sum_{k=2}^{n}(n-k+1) \times \sum_{k'=2}^{n}(n-k'+1)$$

$$= \frac{(l-n+1)(l-n)}{2} \times \frac{n(n-1)}{2} \times \frac{n(n-1)}{2}$$

$$\cong \frac{1}{8}(l-n)^2(n)^4$$

Fig.2 Data sets for the user's habit file.

C. Mining User and Attacker Habits

In this module, a technique called Signature detection technique is used. Signature, in general is used for finding the uniqueness of any individual, thus applying the same ideology the unique behavioural features of a individual helps in finding the attacker by getting alert whenever the uniqueness is deviated. The technique consists of a Host-based security system and network-based IDSs which can discover a known intrusion in a real time manner. It is very difficult to identify the attacker, hence the attack packets are used with forged IPs or attackers may enter a system with valid login patterns. When the user acquires the password, a greater threat may be caused if they try to misuse them. In order to overcome those factors, the signature detection technique helps to reduce the rate of the risks caused even if the passwords are acquired by the victim unfortunately. This concept would be greatly reduces and catches the person with much great accuracy who tries to attack or destroy the confidential data's which belongs to the particular concern.

D. Attacker Analysis and Graph Model

In this module, Host based detection technique is used. This technique consists of the user's forensic features which are retrieved from the user's computer usage history through which the attackers are analysed. Additionally, a security password is to be given whenever any modifications are done by the user who uses it. This, in turn provides a more secured system in a closed environment or an organization where the possibility of threat can be reduced to a greater extent. when any deviations are found, immediately the work is being interrupted by restricting the user from using the system. An attack graph is a modelling tool to illustrate all possible multi-stage, multi-host attack paths that are crucial to understand threats and to decide counter measures. It provides a whole picture of current security situation which can predict the possible threats by correlating detected events. This Attack Graph may appear simple in any successfully running organizationally, since the attackers inside are very hard to find. When the attacker succeeds in attacking, this consequently leads to a great cause successfulness of the concerned organization. So, it is always to be cautious about

the safety and security of the organization by not allowing any of the factors which lowers the progress of the organization.

E. Results and Analysis

The following are the results and analysis of the paper in which the concepts, methodologies, ideologies and different modules used in this paper are analysed sequentially with the help of screenshots, which in turn makes the study of internal attackers more clear. Thus, these are some of the important results and analysis of this work.

Fig.3 Login page for user for authentication.

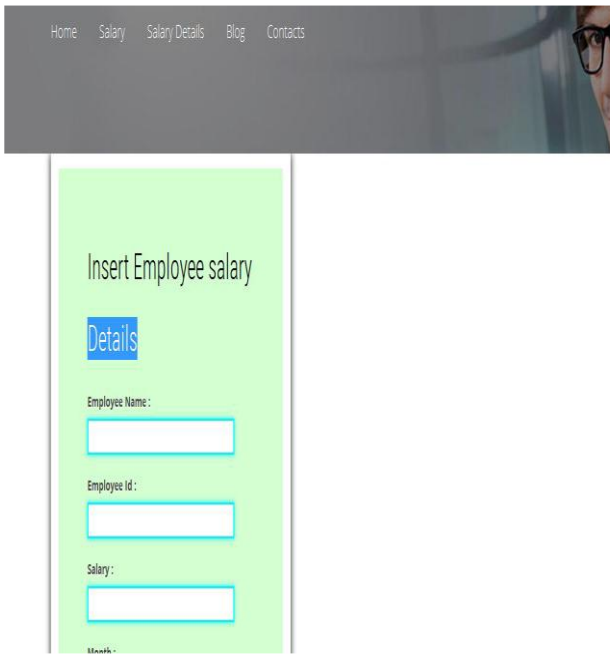
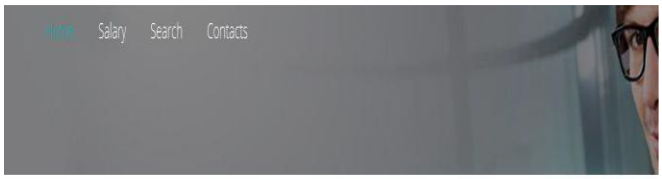


Fig.4.Insertion of the employee salary.



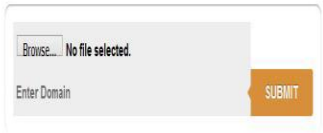


Fig.5. project allocation to the employees.

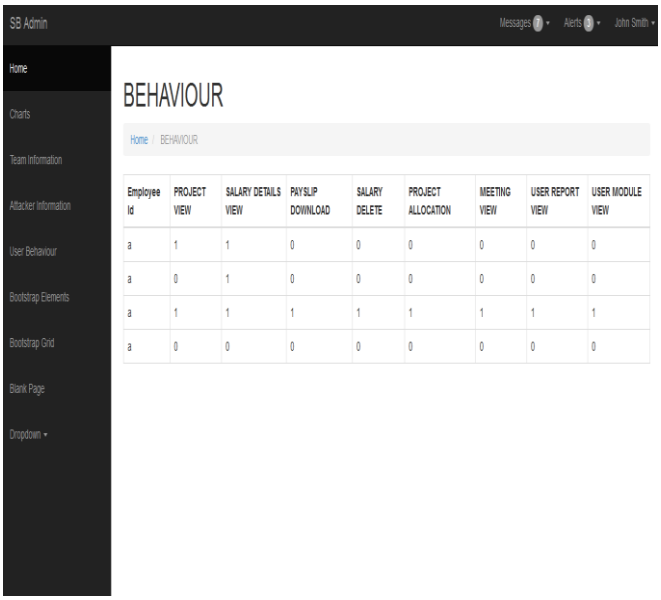


Fig.6. Behavioral table of users.

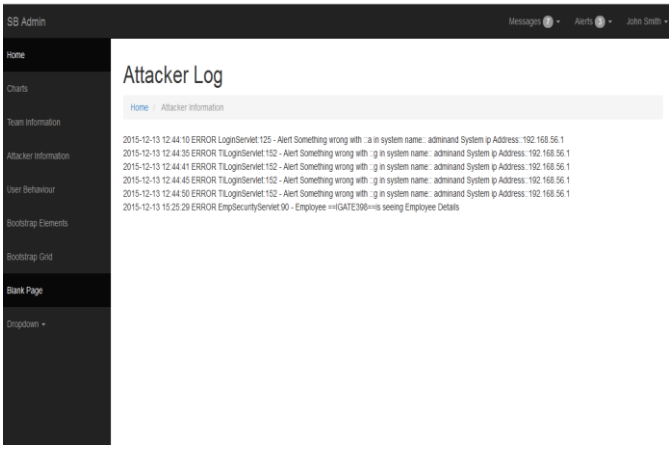


Fig.7 .Attackers Entry Alert Message.

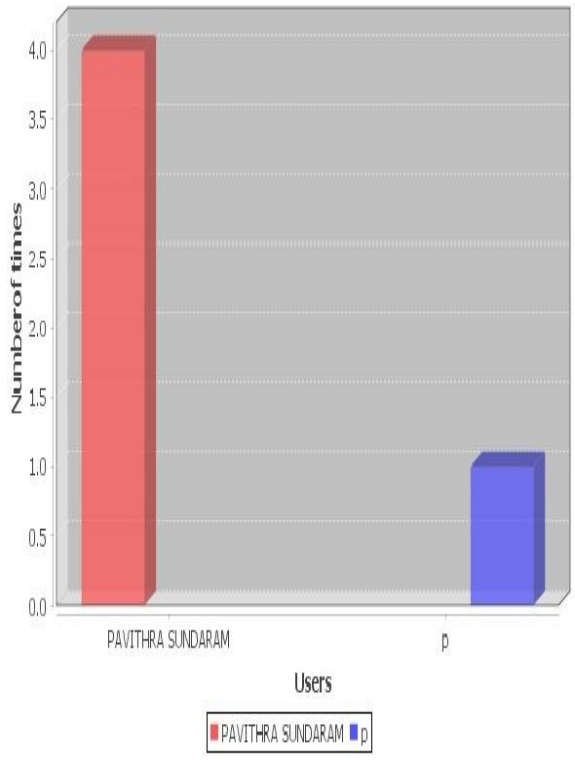


Fig.8 Analysis using Attack graph model.

III. CONCLUSION

In this work, the Sequence which appears in the user's log file is counted and its discrimination score is calculated so that the user's profile can be generated. By comparison with the user's current input usages and commands with the other profiles, the admin can find who the user is. Security passwords on each modifications determines the greater accuracy in detecting the internal attackers who are the most important victims to be found in any closed environment which helps in the progress and growth of the organization. They are highly accurate which makes the effective auxiliary subsystem internally to help in the detection of internal attacks. On the whole, the study on internal attackers in this work would be useful for any organization or institutions in a closed environment to be secured, thereby reducing the rate of risks or any other factor which lowers the progress by the internal attackers.

ACKNOWLEDGEMENT

I thank my **God** and my **parents** first of all, **President, Dr. M.G.R Educational and Research Institute, University** and also I thank **Dr.M.Chandran**, Professor**, Dr. N.JayaChitra, Professor**, Dr. M.G.R Educational and Research Institute, University.

I also thank for the support extended by **Mrs. J.C.Kavitha, H.O.D, CSE**., **Prof.Saradha Devi, Prof. Sarala** and **Prof.S.Maheswari,** , and other friends , P.**Sankari , Sangitha Priya, S.Pavithra,** Dept. of CSE, Meenakshi College of Engineering.

REFERENCES

[1] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in *Proc. Int. Conf.Commun. Soft. Netw.*, Singapore, 2010, pp. 313–317.

[2 J. T. Giffin, S. Jha, and B. P. Miller, "Automated discovery of mimicry attacks," *Recent Adv. Intrusion Detection*, vol. 4219, pp. 41–60,Sep. 2006.

[3] S. Yu, K. Sood, and Y. Xiang, "An effective and feasible traceback scheme in mobile internet environment," *IEEE Commun. Lett.*, vol. 18, no. 11,pp. 1911–1914, Nov. 2014.

[4] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Syst. J.*, vol. 7, no. 2,pp. 262–274, Jun. 2013.

[5] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," *ACM Trans. Int. Technol.*, vol. 10, no. 2, pp. 1–31,May