AN INTRUSION DETECTION AND PROTECTION SYSTEM BY USING DATA MINING FORENSIC TECHNIQUE

**Saurabh Dadhich[1], Ganesh Satpute[2], Anmol Mundra[3], Ruchika Rokade[4],
Prof. Rajashree Karande[5]**

[1,2,3,4](Student)Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Pune, Maharashtra, India, 411041
[5](Professor)Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Pune, Maharashtra, India, 411041

Abstract - Currently, most PC frameworks use client IDs and passwords as the login examples to verify clients. Be that as it may, numerous individuals share their login designs with collaborators and demand these colleagues to help co-assignments, consequently making the example as one of the weakest purposes of PC security. Insider assailants, the legitimate clients of a framework who assault the framework inside, are difficult to recognize since most interruption location frameworks and firewalls distinguish and segregate pernicious practices propelled from the outside universe of the framework as it were. Moreover, a few investigations asserted that breaking down framework calls (SCs) produced by directions can recognize these directions, with which to precisely distinguish assaults, and assault designs are the highlights of an assault. In this way, a security framework, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to identify insider assaults at SC level by utilizing information mining and scientific procedures. The IIDPS makes clients' close to home profiles to monitor clients' utilization propensity. As their forensic features and determines whether a valid login user is the account holder or not by comparing his/her current computer usage behaviours with the patterns collected in the account holder's personal profile.

Key Words: **Data mining, insider attack, intrusion detection and protection, system call (SC), users' behaviours.**

1. INTRODUCTION

In the previous decades, PC frameworks have been broadly utilized to furnish clients with less demanding and increasingly helpful lives. Be that as it may, when individuals abuse ground-breaking capacities and preparing intensity of PC frameworks, security has been one of the major issues in the PC area since assailants more often than not attempt to infiltrate PC frameworks and carry on noxiously, e.g., stealing critical data of a company, making the systems out of work or even destroying the systems. Generally, among all outstanding assaults, for example, pharming assault, appropriated disavowal of-benefit (DDoS), listening in assault, and lance phishing assault [1], [2]. We propose a security framework, named Internal Intrusion Detection and Protection System (IIDPS), which distinguishes pernicious practices propelled toward a framework at SC level. The IIDPS utilizes information mining and legal profiling strategies to mine framework call designs (SC-designs) characterized as the longest framework call grouping (SC-succession) that has repeatedly appeared several times in a user's log file for the user. The client's criminological highlights, characterized as a SC-design much of the time showing up in a client's submitted SC-successions yet seldom being utilized by different clients, are recovered from the user's computer usage history.

1.1 Background

Computer forensics science, which views computer systems as crime scenes, aims to identify, preserve, recover, analyze, and present facts and opinions on information collected for a security event [7]. It analyzes what attackers have done such as spreading computer viruses, malwares, and malicious codes and conducting DDoS attacks [8]. Most intrusion detection techniques focus on how to find malicious network behaviours and acquire the characteristics of attack packets, i.e., attack patterns, based on the histories recorded in log files. These aforementioned techniques and applications truly contribute to network security. However, they cannot easily authenticate remote-login users and detect specific types of intrusions, e.g., when an unauthorized user logs in to a system with a valid user ID and password. In our previous work, a security system, which collects forensic features for users at command level rather than at SC level, by invoking data mining and forensic techniques, was developed. Moreover, if attackers use many sessions to issue attacks.

1.2 Motivation

Most current host-based security frameworks [3] and arrange based IDSs [4], [5] can find a known interruption in a continuous way. Be that as it may, it is exceptionally hard to distinguish who the assailant is on the grounds that assault bundles are regularly issued with produced IPs or aggressors may enter a framework with substantial login designs. In spite of the fact that OS-level framework calls (SCs) are substantially more supportive in distinguishing aggressors and recognizing clients [6], handling a huge volume of SCs, mining pernicious practices.

2. LITERATURE SURVEY

[1] Pritee Shendkar, S. M. Sangv **"New Approach of an Internal Intrusion Detection and Protection System"** International Journal of Innovative Research in Science, Engineering and Technology Vol. 6, Issue 7, July 2017.

In this paper, a security system, called Internal Intrusion Detection and Protection System (IIDPS), is designed to find insider attacks. The IIDPS creates user's habit profiles to keep track of user's habits and determines whether the login user is the account holder or not by comparing the current computer usage behaviours of the user with the patterns collected in the account holder's habit profiles.

[2] Z. B. Hu, J. Su, and V. P. Shirochin **"An intelligent lightweight intrusion detection system with forensics technique,"** in Proc. IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst.: Technol. Appl., Dortmund, Germany, 2007, pp. 647{651. This paper proposed a security system, named the Internal Intrusion Detection and Protection System (IIDPS) to detect insider attacks at SC level by using data mining and forensic techniques in networked data. The IIDPS creates users' personal profiles to keep track of users' usage habits as their forensic features and determines whether a valid login user is the account holder or not by comparing users current computer usage behaviours with the patterns collected in the account holder's personal profile. The idea behind the inside attacker detection in wire-less sensor network by exploiting the spatial correlation between the packet ratio, which help to detecting dynamic attacking behaviours The routing is performed to identify the shortest path between each source node and their destination address and residual energy is calculated for each node in the network.

[3] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, **"Data-stream based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study,"** IEEE Syst. J., vol. 9, no. 1, pp. 1{14, Jan. 2014.

In this paper security System defene s as the Internal Intrusion Detection and Protection System (IIDPS), is help to detect internally attacks by using data mining and forensic technique at SC level. For the track the information of users usages the IIDPS creates users' personal profiles as their forensic features and investigate that the valid login user is account holder can login or not by comparing his/her current computer usage behaviours with the patterns collected in the account holder's personal profile. The experimental results demonstrate that the IIDPS's user identification accuracy is 94.29.

[4] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, **"Detecting web-based DDoS attack using MapReduce operations in cloud computing environment,"** J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28{37, Nov. 2013.

This paper proposes a method of integration between HTTP GET flooding among DDOS attacks and MapReduce processing for a fast attack detection in cloud computing environment. This method is possible to ensure the availability of the target system for accurate and reliable detection based on HTTP GET flooding. In experiments, the processing time for performance evaluation compares a pattern detection of attack features with the Snort detection. The proposed method is better than Snort detection method in experiment results because processing time of proposed method is shorter with increasing congestion.

3. EXISTING SYSTEM

In the current framework client IDs and passwords as the login examples to confirm clients. Be that as it may, numerous individuals share their login designs with collaborators and demand these associates to help co-undertakings, subsequently making the example as one of the weakest purposes of PC security. Insider aggressors, the legitimate clients of a framework who assault the framework inside, are difficult to recognize since most interruption identification frameworks and firewalls distinguish and detach malignant practices propelled from the outside universe of the framework as it were.

Disadvantages of Existing System

1. To authenticate the system with just login and password is inefficient.

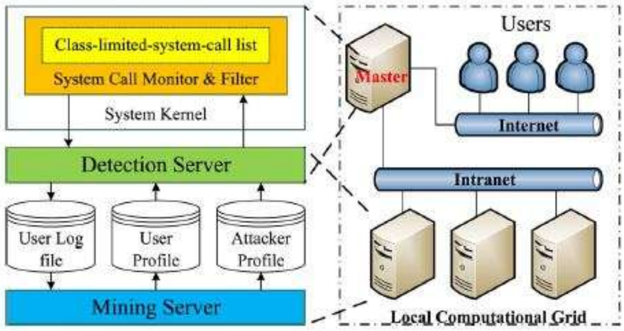
2. It cannot able to find the intruder in the internal system.

4. PROPOSED SYSTEM

The IIDPS, as appeared in Fig., comprises of a SC screen and channel, a mining server, a location server, a nearby computational matrix, and three storehouses, including client log records, client profiles, and an assailant profile. The SC screen and channel, as a loadable module inserted in the part of the framework being considered, gathers those SCs submitted to the bit and stores these SCs in the configuration of uid, pid, SC in the secured framework where uid, pid, and SC individually speak to the client ID, the procedure ID, and the SC c put together by the fundamental client. It likewise stores the client contributions to the client's log record, which is a document keeping the SCs put together by the client following their submitted arrangement. The mining server investigations the log information with information mining methods to distinguish the client's PC use propensities as his/her personal conduct standards, which are then recorded in the user's profile.

Advantages of Proposed System:

1. Can distinguish a client's measurable highlights by dissecting the comparing SCs to upgrade the precision of assault recognition;
2. Able to port the IIDPS to a parallel framework to additionally abbreviate its identification reaction time; and
3. Effectively oppose insider assault.



5. CONCLUSION

We have proposed an approach that employs data mining and forensic techniques to identify the representative SC-patterns for a user. The time that a habitual SC pattern appears in the user's log file is counted, the most commonly used SC-patterns are filtered out, and then a user's profile is established. By identifying a user's SC-patterns as his/her computer usage habits from the user's current input SCs, the IIDPS resists suspected attackers.

6. REFERENCES

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers Or how to thwart a phisher with trusted computing," in Proc. IEEE Int. Conf. Avail., Rel. Security, Vienna, Austria, Apr. 2007, pp. 120–127.

[2] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," ACM Trans. Int. Technol., vol. 10, no. 2, pp. 1–31, May 2010.

[3] Q. Chen, S. Abdelwahed, and A. Erradi, "A model-based approach to self-protection in computing system," in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL, USA, 2013, pp. 1–10.

[4] F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, "Detection workload in a dynamic grid-based intrusion detection environment," J. Parallel Distrib. Comput., vol. 68, no. 4, pp. 427–442, Apr. 2008.