Journal of Science and Technology
ISSN: 2456-5660 , Volume 06, Issue 01, Jan-February 2021

www.jst.org.in *DOI: https://doi.org/10.46243/jst.2021.v6.i1.pp141- 147*

A Highly Accurate Internal Intrusion Detection and ProtectionSystem Using Time Linked Access Profiles

Veena P[1], SyamDev R .S[2]

[1](Computer science and Engineering, Narayanaguru college of Engineering, India)
[2](Computer science and Engineering, Narayanaguru college of Engineering, India)
[1]Corresponding Author: veenapadma@gmail.com

To Cite this Article
Veena P and SyamDev R .S, "A Highly Accurate Internal Intrusion Detection and ProtectionSystem Using Time Linked Access Profiles"", Journal of Science and Technology, Vol. 06, Issue 01, Jan-February 2021, pp141-147

Article Info
Received: 14-09-2020 Revised: 25-12-2020 Accepted: 04-01-2021 Published:08-01-2021

Abstract:*Because most intrusion detection systems and firewalls identify and separate malicious traits that only come from the external environment of the system. It is difficult to differentiate between the actual system users, the internal attackers who access the device.Also, studies claim that these commands can be recognized by analyzing the system calls produced by these commands.This system, therefore, includes an Intrusion Detection and Protection System (IDPS) security system to detect internal attacks on the System Call (SC) using data mining and forensic techniques.However, some attacks have improved their method, further providing security and preventing the user from tracking user access profiles and patterns. In this work, a new technique is proposed to prevents profile attacks by disconnecting access patterns from users for a specified period based onTime Linked Access Profiles (TLAP). To evaluate the performance detection accuracy is calculated and it is improved when compared to the convolution neural network.*

Keywords*:Intrusion Detection Systems, System security, Time Linked Access Profiles, Central Processing Unit, Message Passing Interface, Virtual Machines, Distributed Denial of Service*

I. Introduction

Computer systems have become common in recent decades, providing users with an easy, comfortable, and efficient life. However, when people use the powerful tools and computational capacities of computer systems, security is a major concern in the computer sector, so criminals often try to exploit computer systems, such as stealing confidential company data or even breaking systems.In any aspect of any real system, the internal threat is a major problem where access to sensitive and confidential information can be misused and compromised by access authenticators; or cooperate with others to cause system interruption, harm, and serious harm to the system[1].As firewalls and intrusion detection systems (IDS) typically defend against external threats, an internal attack is one of the most difficult to detect. The user ID and password are verified by most systems as a login template for authenticating users. Trojans can, however, be installed by attackers to steal login templates from the victim or to execute large-scale dictionary checks to obtain user passwords. They can log in to the system, access the private files of users, and change system settings if successful. Fortunately, in real-time, most modern host-based security systems and network IDS can detect known intrusions. However, since attack packets are often sent with false IP addresses, or attackers may log in with appropriate login patterns, it is very difficult to identify who the attacker is.While system calls are more useful for user detection and identification at the Operating System (OS)level large-scale SC exploitation, malicious detection, and identification of possible intruders are still engineering problems[2].Trojan horses may be inserted by internal attackers, scan the network file system, overload the system, or cause system crashes. It directly impacts the availability of the system's network. Unfortunately, such attacks can be very difficult to find or prevent without adequate detection and security systems. Although various computer or network systems that have different security principles, authentication or identification, encryption, and access control are used for early attempts at security systems.These systems aim to prevent unauthorized users from gaining access to and protect against denial of service, data confidentiality, data integrity, and communication. It has been

found that the protection of protected systems cannot be ensured by such defense-based approaches. (DDOS) Distributed Denial of Service attacks, for example, blocked the normal functioning of many major commercial sites in 2000, including Yahoo and CNN, although they were covered by defensive methods[3]. To identify breaches of security policies of the device. Intrusion detection does not replace safety measures such as authentication and access control but instead seeks to work with system security controls to overcome existing security limitations. It is also common to see infiltration detection as the second line of protection against computers and networks. The issue of identification is to identify users, hosts, or applications who use the computer system without permission, as well as those who have legal access to the system but are manipulated by their ancestors. Several kinds of infiltration detection methods are used. Adapting the IDS to identify internal attacks can be challenging.Part of the challenge for IDS is to build a good recognition engine. Because of the difference in the method of identification, different network users require different amounts of access to operate various services, servers, and systems. System administrators may identify any network users who, if any attack patterns or activity is identified[4], pose a threat to network or system protection. An internal threat also exists and it manifests itself in different ways.In light of changing technical, social, business, and cultural factors, internal threats need to be handled. Experience has shown that over-reliance on technology, regardless of other factors, can have devastating consequences in all circumstances, especially when searching for "alert signs," for dealing with the internal threat addressed. It is important to note that there are no significant adverse effects from malicious attacks, such as accidental loss or knowledge leakage. An attacker can do more harm to an organization from within and has several advantages over an external attacker because the attacker has legitimate and advantageous access to property and documents, knows the procedures of the organization, and insiders know how to attack and how to cover their tracks, and when to attack. Outsiders need to target and collect multiple information sources before they can work, while an insider can specifically target information and not have to overcome any of the problems faced by an external intruder[5].
It would be very evident from the above discussion that locating intruders is the most difficult thing. Fortunately, most modern host-based security systems and network IDS can detect known intrusions in real-time.This paper suggests a new way to boost the intrusion detection and system's efficiency. This is done by using the new method that prevents profile attacks by disconnecting access patterns from users for a specified period based on TLAP. The subtitles of the proposed strategy are clarified in the following area.The organization of the paper is as follows;Section II provides details of previous actions taken to detect intrusion systems. Section III describes a summary of the proposed ambiguous decision-making method. Results and discussion with intrusion detection are given in IV. Finally, Section V concludes the article.

II. Literature Survey

Previously, various techniques have been proposed to perform the intrusion detection process. The maximum of the techniques is focusing to perform and to detect the intruder with various techniques. Some of the previous techniques which are used to perform the intruder with less time delay are explained in this section.

Hongtu Li, et al., (2011) proposed that by adding password authentication services to Horg's non-authenticated multilateral key contract protocol, the dictionary suggested a key password-based password management protocol that is effective against attacks. They argued that the proposed protocol was very successful because a session key needs only persistent conversation rounds, and each user exchanges persistent messages and only four explanations are needed. According to the Diffie-Hellman hypothesis, both the compatible cipher model and the random Oracle model were secure with the unique protocol[6].

Sameera Mubarak and Jill Slay(2009) stated when the law firm was invited to research the attitudes of lawyers towards computer security and the potential to hack their trust accounts. Simultaneously, this explores whether a large amount of evidence can support the patterns found in the case studies. The overall result highlights the fact that law firms did not have the latest cybercrime technologies. From a human point of view, more concerns have been reported, such as the lack of computer system monitoring and the inadequacy of access control. The findings indicate that security policies need to take immediate security action, enact information security policies and procedures, and work with officials to organize these policies[7].

Jan Platos, et al.,(2009) proposed that the majority should pay attention to the riskier defense from external threats.Industry study has internally recorded assaults. An uncommon form of threat that is severe and very common is internal attacks. Unlike an external intruder, an intruder is someone who trusts allowed network access in an internal attack. This introduces a method of non-negative matrix factorization for internal attack detection. The non-

negative matrix factorization method shows that it can be an ideal candidate for detecting internal threats, compared to other widely accepted pattern recognition technologies[8].

Kuheli Roy Sarkar, (2010) proposed the internal threat is more confusing than any other threat. The first step in assessing the likelihood of an internal attack is internal threat assessment. Technical solutions are not adequate since there are mostly human issues with internal threats.Therefore, technical, behavioral, and organizational assessment is a three-step approach to facilitate the prediction of internal threats and prevent internal attacks, thereby enhancing the security, survival, and re-establishment of the organization in light of internal threats[9].

Wenbo Shi proposed,(2009)an intrusion detection system used by file integrity analyzers and a mobile intrusion detection agent, which has been suggested to detect malicious internal activity. Safety flaws and malicious platforms can easily compromise sensor agents in the lower eclipse. A protection mechanism called the Confident Clone Agent Protocol is then integrated. Although there are multiple malicious platforms, the confidential structure has been improved to protect these agents, strengthen their security, and complete their calculations and locate malicious hosts[10].

However, the above-mentioned methods have merits and demerits. The main disadvantage of the previous works is to improve the detection of the intruders and protection from them. The main purpose of this article is to overcome the shortcomings of the previous work. In the detection of malicious insider attacks and their causes, there are different methods.

1. This paper suggests an improvement in the security of distributed data networks.
2. To reduce the complexity of the process of detection, which improves the potential of the process of real-time testing.

The details of the implementation of the proposed work are given below sections.

III. Proposed Method

To recognize malicious activity leading to the device, a security system called the Internal Intrusion Detection and Protection System (IDPs) is intended. To speed up the identification and mining of intrusion detection and protection systems and to enhance their detection and mining capabilities, the discovery server and mining server run mostly on a local area network.If a user logs in with the login pattern of another person, IDPS effectively identifies the user by calculating the similarity scores between the user's current inputs i.e. the SC and the activity stored on different user profiles[11]. The use of different user groups of classes in the base system in the IDPS list, which is stored as the main component of the SC monitor and filter in the SC limited class list, is prohibited for SC, i.e. such privileges cannot be extended by the administrator. As a result, the commands created by these system calls will be barred from using all privileges.

Many challenges were created and quite enough to track the access patterns of users. To give more security and to prevent tracking of user access profiles the proposed IIPDS is enhanced with a novel scheme called TLAP. The new method prevents profile attacks by delinking the access patterns from the users after a period based on TLAP. In this advanced system for each user, the access patterns or SC are activated with the help of Time Linked Access Profiles or Patterns algorithm. During which the validity of the pattern is decided by the TLAP time frame, such that the user's patterns lifetime is controlled by the TLAP parameters or threshold, when the threshold reaches the system clears the access patterns and prevents the user from system access.

Internal Intrusion Detection and Protection System Architecture: The attacker-specific pattern or the attacking pattern (or signature) that the attackers commonly use can be identified in the way that, of an IDPS method. An attack pattern is often presented by an attacker, but is rarely considered one of the most common attack patterns and is not sent by others and gains high closeness. It is also possible to categorize signatures obtained on an attacker's profile as normal signatures and attacker-specific signatures.

Block Diagram:In the insider attack detection, inappropriate use of the devices, network data breaches, device theft or loss of device with data, or lack of education of the employee to enclose the sensitive data within are the specific errors that are made generally. The detection avoidance technique prevents these attacks by checking the threat agent to be suspicious and update the user profile and during the validation of the next process based on it. As shown in the figure.1 If a system call is found to be suspicious it will be sent to the defender component.

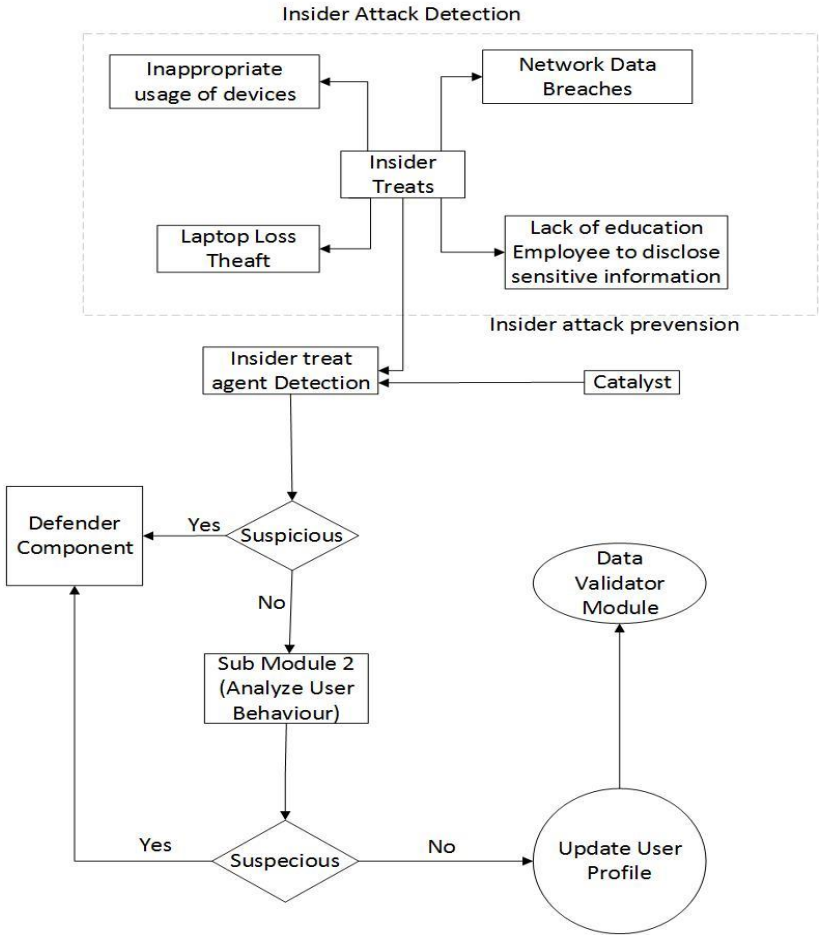

Figure.1Block diagram for the proposed system

Parameters Considered:

1. SC monitor and filter
2. Discovery server
3. Mining server
4. Local computing grid

Included in IDPS are all parameter sets, including the SC monitor and filter, mining server, discovery server, local area network, user log files, user accounts, and attacker profile. These SCs are collected and filtered by the SC monitor and sent as a loadable module to the kernel mounted in a suspicious device kernel and stored in the user id (UID), process (PID), and SC protected system formats, where the user IDs are UID, PID, and SC. It also stores user input in a log file for users, which is a file that stores user-sent tables. The mining server uses mining techniques to analyze log data, classify the computer use habits of the user actions, and then record them in the profile of the user[12]. The monitoring server compares the attacker's malicious activity and real-time identifier with the SC patterns, attack patterns, and patterns collected on the attacker's profile in the user profile. The SC monitor filters are detected when an intruder is identified and alerted by the detection server to isolate the user from the safety device. The aim is to prevent invaders from continually attacking the system.

Intrusion detection and monitoring system using the proposed technique: To speed up IDPS online detection and mining, as well as enhance detection and mining capabilities, the discovery server and mining server run on the local area network. When a user logs in with the login pattern of another person, IDPS identifies the user effectively by measuring the similarity scores between the current input of the user, that is, the SC, and the habits stored in the

profiles of different users.There are system calls and system procedures in the IIDP 'S, which is stored as the main component of the SC monitor and filter in the restricted class SC list, which are forbidden for use by various user classes in the basic system, e.g. the admin should not submit SCs with so many special statuses. As a result, all admin will be barred from using the commands generated by this system calls[13]. To provide more security and prevent tracking of user access profiles, specific IDPS has been enhanced with a new scheme called TLAP. The new method prevents profile attacks by delinking the access patterns from the users after a period based on TLAP. In this advanced system for each user, the access patterns or system calls are activated with the help of Time Linked Access Profiles or Patterns algorithm. During which the validity of the pattern is decided by the TLAP time frame, such that the user's patterns lifetime is controlled by the TLAP parameters or threshold, when the threshold reaches the system clears the access patterns and prevents the user from system access.

In Figure.2, a system model is shown with a system call flow. The relationship between the detection server, mining server, and local computational grid in the data recovery domain is identical to the relationship between the SC and the kernel command that the attacker produces. To measure the weight of the SC frequency generated by the kernel, the term frequency (TF) is defined as.

$$TF_{i,j} = \frac{p_{i,j}}{\sum_{l=1}^{l=h} p_{i,j}}$$

Where, $p_{i,j}$ is the number of systemcalls and$l$ is the limit 1 to h

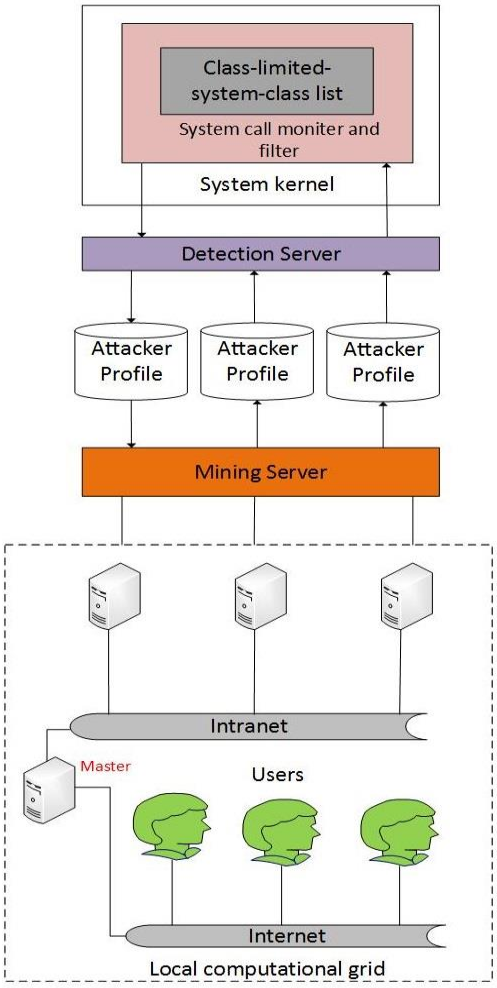

Figure.2 System model with control flow of system calls

Types of Attacks: Three kinds of intrusions are detected from this method. Type I is the use of community members as a scenario in which an SC is submitted by the recipient of a specific group is prohibited. Type II attack is a sensitive SC attack that can alter system environment parameters, attack the system, or delete or adjust sensitive data or system parameters. Type II attack is a sensitive SC attack. The type III attack is made up of SC layer attack patterns, i.e. SC patterns, which are all considered a point of attack. Often an aggressor combining a particular system calls will successfully reach a safety system.

IV. Results and Discussions

Three experiments were conducted to assess the feasibility and precision of IDPS. The first determines the crucial limit of velocity between the user profile that hasbeen set up and the profiles of each other. The second was to check the reliability of the online discovery server when it was sent to NCSU. Thirdly, IDPS has been compared with many modern host-based IDS (HIDS). The front end used in this proposed method is HTML and the oracle database is used to store the data. The outcome extends the characteristics of data mining and forensic techniques used for intrusion detection to provide successful resistance to attacks. The legality of a login user can be defined by the IIDP.

Decisive Rate Threshold: This experiment has been conducted ten times. If the similarity score is stated above or between the limits and user profile, if the similarity score between upper the limits and 7 user profiles is 100% secured, then the known user is given the currently scheduled input sequence, i.e., the limit is the critical rate range from the table.

Detection Accuracy: Hundreds of thousands of SCs will be created when a user inputs an order. It also takes a long time to evaluate a large number of SCs. IDPS spends 0.45 s on the identification of a recipient. While other systems take more time than IDPS for data processing, the objective is to get equal scores for all users so that IDPS can decide on the intranet users. Statistical information for the 12 user profiles built by the Mining Server, which displays the User ID “Number ID”, Number of SC templates collected in the user profile. 40% of normal user templates have been removed because their similarity weight is less than the default limit of 0.001.

Table no 1: Shows Identification accuracy of proposed IDPS

Account ID	No of Paragraph	Times of being an account holder	Times of being an attacker	Detection Accuracy
Root	116	110.03	5.24	92.13
Oracle	117	120.20	6.23	93.22
Reservation	182	94.46	19.15	95.69
Financial	220	206.32	12.33	95.15
Backup	62	62.32	4.25	95.64
Business	146	165.23	9.22	85.23
Audit	110	105.98	7.95	96.74
Average	136.142	123.5057	9.195714	93.4

In Table no 1, no of the paragraph is the number of times the user's test data should be considered for the decision rate, “time of being account holder” is ten times larger than the predetermined limit of this determination factor, and if the critical dimensions are less than the predetermined limit, the attacker is the current user. The "attack time" is the average time that the system administrator is alerted to 10 times its value. "Accuracy of detection" is the accuracy of verifying the identity of a user. A framework for managing databases used to store and process data in SQLite. Using less than 1 GB to store user accounts, IDPS have 100 GB of drums and 10 TB of hard drives.

Comparison of IDPSwith Other HIDSs: To detect possible threats, HIDS also gathers and analyses the information provided by device users. A third experiment compared IDPs to four HIDs to examine the infiltration detection capabilities of the device. It has a collaborative learning agent that analyses log files to identify basic Type III attacks. For the specified time, Tripwire checks the security of the files and directories of the system administrator. It detects DDOS attacks caused by the system by monitoring the traffic going out of the system. False alarms may also be caused, especially when users or regular programs upload data to the internet.

Table no 2: ShowsComparison of IDPS with other HIDS

Security System	Attack type / response time (second)				
	Identify User	Type 1	Type 2	Type 3	DDOS
OSSEC[14]	No / -	Yes / 60	Yes / 60	No / -	No / -
AIDE[15]	No / -	Yes / 60	Yes / 60	No / -	No / -
IDPS	Yes / 0.45	Yes / 0.01	Yes / 0.01	Yes / 0.45	Yes / 0.45

Type I attack is an attack that forbids the use of a certain group. Type II attacks are used to provide sensitive SCs for the transfer of sensitive data and device resources. The software uses IDPS, a program monitoring tool, to track the progress of the Type III attack, and launches a diode attack to attack external device response times for all types of attacks, as seen in Table No 2, in which IDPS outperform thanother tested systems.

V. Conclusions

In this work, a new technique approach with profile attacks, the problems generated are enough to track user access patterns. A new method TLAPs aims to prevent the tracking of user access profiles on a specific system. Experimental analysis has shown that profile attacks can be prevented by disabling access patterns from users for a specified period based on TLAP. The experimental results show the detection accuracy of IDPS higher than 93%. The proposed system works excellently and safety is optimized with the new system.

References

[1]. Leu,Fang-Yie, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao-Tung Yang. "An internal intrusion detection and protection system by using data mining and forensic techniques." IEEE Systems Journal 11, no. 2 (2015): 427-438.
[2]. Song,Jinwoo, and Young Moon. "Security Enhancement Against Insiders in Cyber-Manufacturing Systems." Procedia Manufacturing 48 (2020): 864-872.
[3]. Bu, Seok-Jun, and Sung-Bae Cho. "A convolutional neural-based learning classifier system for detecting database intrusion via insider attack." Information Sciences 512 (2020): 123-136.
[4]. Colwill, Carl. "Human factors in information security: The insider threat–Who can you trust these days?." Information security technical report 14, no. 4 (2009): 186-196.
[5]. Elmrabit, Nebrase, Shuang-Hua Yang, Lili Yang, and Huiyu Zhou. "Insider Threat Risk Prediction based on Bayesian Network." Computers & Security (2020): 101908.
[6]. Li, Hongtu, Liang Hu, Wei Yuan, Hongwei Li, and Jianfeng Chu. "Insider attack on a password-based group key agreement." Procedia Engineering 15 (2011): 1700-1704.
[7]. Mubarak, Sameera, and Jill Slay. "Protecting clients from insider attacks on trust accounts." Information security technical report 14, no. 4 (2009): 202-212.
[8]. Platos, Jan, Vaclav Snasel, Pavel Kromer, and Ajith Abraham. "Detecting insider attacks using non-negative matrix factorization." In 2009 Fifth International Conference on Information Assurance and Security, vol. 1, pp. 693-696. IEEE, 2009.
[9]. Sarkar, Kuheli Roy. "Assessing insider threats to information security using technical, behavioural and organisational measures." information security technical report 15, no. 3 (2010): 112-133.
[10]. Shi, Wenbo, Injoo Jang, and HyeongSeonYoo. "An inside attacker proof intrusion detection system." In 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, pp. 1020-1024. IEEE, 2009.
[11]. Inayat, Zakira, Abdullah Gani, Nor BadrulAnuar, Shahid Anwar, and Muhammad Khurram Khan. "Cloud-based intrusion detection and response system: open research issues, and solutions." Arabian Journal for Science and Engineering 42, no. 2 (2017): 399-423.
[12]. Yin, Chunyong, Luyu Ma, and Lu Feng. "Towards accurate intrusion detection based on improved clonal selection algorithm." Multimedia Tools and Applications 76, no. 19 (2017): 19397-19410.
[13]. Shterenberg, S. I., and Maria A. Poltavtseva. "A distributed intrusion detection system with protection from an internal intruder." Automatic Control and Computer Sciences 52, no. 8 (2018): 945-953.
[14]. OSSEC. [Online]. Available: http://www.ossec.net/
[15]. AIDE. [Online]. Available: http://aide.sourceforge.net/