International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Privacy Protection Against Insider Attacks

M Rama Bai, Maaz Bin Saad Quraishi

Abstract*: *A growing number of public and private sector organizations are recognizing insider threats as a critical area. In response, many steps are taken to defend assets against risks posed by employees and third-party trust. Insiders pose unique challenges for defenders. Traditional security tools are unlikely to audit insiders, let alone privileged users who have a potentially malicious intent. Although a high-risk activity, it is common to see users sharing passwords between colleagues or subordinates, defeating the purpose of authentication. This increases chances of Insider Attacks (IA), as it is hard to identify malicious insiders, given an attacker is entrusted with highly privileged access to read and write operations. Information Technology Organizations employ many workers with varying level of access, and every user is authenticated with unique login credenti¬als. Controls need to be put in place in order to secure the systems, since it can hamper login patterns. Research indicates that by analysis of system calls (SCs) that are generated upon user login can detect intrusions and read such patterns that are against the normal operations of the system. Information Technology Organizations employ many workers with varying level of access, and no two users have same login behavior. Given every user has a unique login pattern, this work proposes a system called Privacy Protection Against Insider Attacks (PPIA) which learns the login pattern of each user that is authenticated and employs data mining concepts to read user behavior and endeavors to detect insider attacks .Experimental results indicate that the approach is very effective and accurate..

Keywords* : *Inside Attacks, Privacy Protection of Inside Attacks, DoS & DDoS.

I. INTRODUCTION

Popular computer system and network attackslike Denial of Service(DoS), Distributed Denial of Service(DDoS) and teardrop attacks – referred to as outside attacks are relatively easier to detect. When a data transfer is initiated and leaves the perimeter of an organization, a network attack can occur. There is a plethora of solutions for such types of attacks and there is ongoing research for detection and protection of such attacks. In general, organizations havemany employees, and many teams require users to share a common user account in order to perform daily tasks. Chances of misuse of the account increase exponentially when multiple people in a team share a common password. Moreover, when someonemakes it into a user account, it is easy for them to misuse it and perform read and write operations without anyone's notice. Such attacks are what we refer to as Insider Attacks, and the person performingan Insider Attack is called Inside Attacker. It is very difficult to find the inside attacker in the real time, because system exists to track the user operations. Track all user behaviors is critical, and when a user operation does not match with existing user behavior the system should respond and alert the actual user. This work proposes a concept called Privacy Protection Against Inside Attacks (PPIA) and aims to achieve a solution to insider attacks. No two users have same user behavior, and hence the goal is to monitor the users' behaviors (habit data) by collecting the System Calls (SC). System Patterns are formed on the basis of System Calls, and basis these patterns detection of insider attacks is achieved. For this we are proposing a novel architecture with the help of the traditional data mining techniques.

II. RELATED WORK

In the current system, there is no work for insider attacks, only focus is on the network based attacks. Network attacks like DoS, DDoS and teardrop attacks, can be referred to as external attacks. Solutions exist that address the external attacks andthere is ongoing research being performed by security companiesand are coming up withsolutions toissues erupting in the network-based attacks arena. Zhiyong Shan et al. proposed a Secom [1] architecture for securely accessing and committing operations in virtual systems at the OS level. A virtual machine can be spun up with minimal cost and is highly scalable given it shares the host's resources. It is a perfect arena for fault tolerance and intrusions - which allows users to trial new applications and not having to worry about malware. Secom concept is to find and observe the operations performed in a virtual machine and revert malicious changes that have been done to the system, before they are committed at the OS level. When sensitive operations are processed on the servers like commit, deploy, or delete data on a database, a verification operation can be generated before it is processedin the Operating System. In other words, Virtual Machines require that data is securely committed thereby allowing only genuine changes in the host environment and filter out any changes that have been performed with illicit intentions. J. Choi et al. described DDoS attacks in the web-based applications by using the session-based HTTP protocols like GET or POST. These protocols have a potential toallow the malicious traffic to reach targeted web servers, for which the target system is unprepared for. In this study, they proposed a concept by monitoring the traffic of a HTTP request using Map Reduce concept for fast monitoring and reliable detection [2].

Revised Manuscript Received on May 28, 2020.
* Correspondence Author
M Rama Bai*, M-Tech, Dept.:-CSE, Mahatma Gandhi Institute of Technology, GANDIPET, HYDERABAD, TELANGANA, Mail Id:- maazsq@gmail.com
Maaz Bin Saad Quraishi, Professor, Dept.:-CSE, Mahatma Gandhi Institute of Technology, GANDIPET, HYDERABAD, TELANGANA, Mail Id:- rama@mgit.ac.in

Kang et al. proposed a concept of IP traceback [3], wherethe approach two-fold; for every request that is analyzed, in addition to performing traceback, a communication is generated for other security systems by means of logging methods. Karen et al. described concept called PID (Postmortem Intrusion Detection), which includes detection system of the internal intruders by taking the log files of the user behavior after the attack. Log file consisting of a sequence of operations is collected, and a classification algorithm to predict the pattern of the user behavior is applied in terms of the sequence of the operations. To process the attacker log operations, a cluster technique is used, and k-means approach for clustering the user log file operations after the attack is proposed. In their work, the process consists of two steps; one is sliding window and another on the detection model. The sliding window system splits and groups the user log files operation with different types of intervals. Next detection model performs the classification technique and separatesnormal and malicious behavior, where behavior refers to sequence flow of the operations in the log files.

III. IMPLEMENTATION

The algorithm below depicts how a server extracts the system call sequence that is generated when a user logs in and count the number of times that a specific SC-pattern appears.

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 ≤ G−1 ; i++) {
3.    for ( j=i+1 ; j ≤ G ; j++) {
4.      for (each of ∑_{n=2}^{|Sliding window|}(|Sliding window| − n+ 1) n-grams in
          current L-window){
5.        for (each of ∑_{n'=2}^{|Sliding window|}(|Sliding window| − n' + 1) n'-grams
            in C-window){
6.          Compare the n-grams and n'-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 for generating user habit file

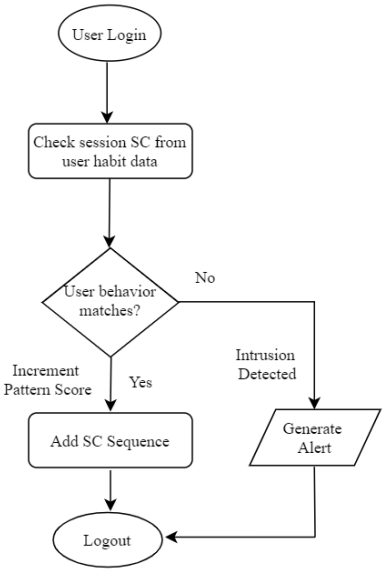

Fig.2. Information Flow

The figure above depicts how a mining server extracts a system call sequence from the log file when a user logs in and counts the number of system call patterns in the file and stores it in the habit file.

Architecture

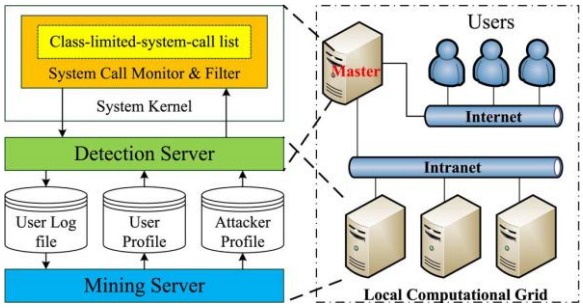

Fig.3. Architecture

PPIA

PPIA is an application which represents the concept called Privacy Protection Against Insider Attacks, to tackle run over Internal Intrusions and interior gatecrashers. To validate clients, at present, this work structures an investigationby utilization of login test by client recognizable proof and secret word. Thisapplication tracks the user behavior in a few steps. Initially, when user logs into the application, the system tracks the user's operations and order in the sequence, using a concept calledn-gram technique, which analyzes the series and sequence of the system calls and generates the system pattern.

Detection and Protection

The application keeps track of the user operations in the form of system calls. For example; when a user initiallylogs inand updates his profile, the system calls generated are open, view, update etc. Based on these system calls,the application generates the SC patterns.

User Process

Auser is a co-worker in a set of personnel in an enterprise, consumer can log into device the usage of their own login sample.After logging in, a user performs operations like upload, download, replace, ship, view and so on. Application user can receive an alert by configuring the alert, upon attack.

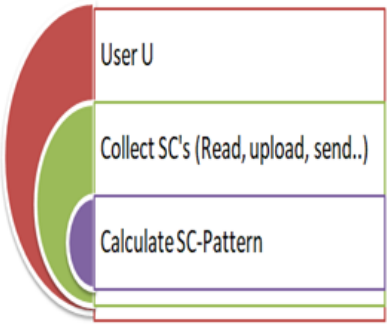

Fig.4. User Process

Admin

Admin is the main actor of the system who monitors the system patterns by selecting the individual user accounts. Admin can see the list of the attacks.

The alert generated describes the properties of an attack like victim user, attacker information, level of the attack whether it may be type I, II, or III. Admin also monitors the source of attack and can trace the attacker using the IP address of the attacker machine.

User

User is the normal end user who does routine operations according to the assigned rights. User's behavior or habits are based on the position and work assigned. The user would receive an alert through emailupon attack initiation on the account. Basis the alert, the user can react and revoke the operations initiated by the attacker.

Attacker

Attacker is a malicious person who logs into others user accounts with valid correct login details. Based on the user habits and system calls generated, the system detects the attack and level of the attack.

System

Our system monitorsthe system calls of the users. It prepares the system pattern based on the system callsequence. If a user accesses the system and the generated system calls do not match the existing system pattern, then system raises an alert via email, leaving it to user's discretion to revoke the operations made by the attacker.

IV. EXPERIMENTAL RESULTS

The following page consists of register inputs and all the details are given by user and click on the register that should be stored in database for it to be used for login.

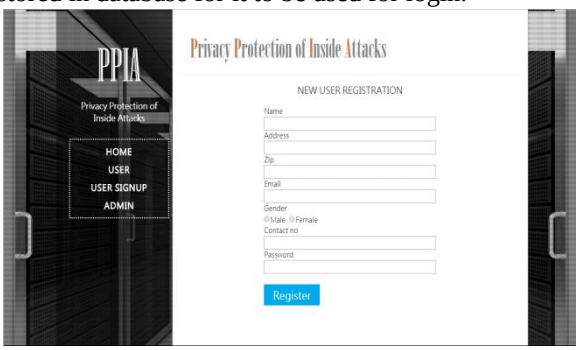

Fig.5.Register Input

Fig.6.File upload

The file is uploaded in the above format. File is in txt format with keywords and it gets stored in the database.

V. CONCLUSION

This research achieves detection and protection system of insider attacks by proposing a concept called Privacy Protection Against Insider Attacks (PPIA). The proposed architecture is to secure the user accounts and data when user account is attacked by the attacker. It is very difficult for multiple users to have the same behavior. Therefore,this work monitors the user's behaviors and habits by collecting the System Calls (SC). Based on the System Calls,a system pattern is prepared. Based on the created patterns, a detection mechanism against insider attacks is achieved. This work proposes an architecture with the help of n-grams and profile matching algorithms.

REFERENCES

1. Z. Shan, X. Wang, T. Chiueh, and X. Meng, "Safe side effects commitment for OS-level virtualization," inProc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120.
2. 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
3. H. S. Kang and S. R. Kim, "A new logging-based IP traceback approach using data mining techniques,"J. Internet Serv. Inf. Security,vol.3, no. 3/4, pp. 72–80, Nov. 2013
4. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N.J. Peterson, D. X. Song, Provable data possession at untrusted stores.ACM Conference on Computer and Communications Security, 598-609,2007.
5. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner,Z. N. J. Peterson, and D. Song, Remote data checking using provabledata possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.
6. A.Juels, and B. S. K. Jr. Pors, proofs of retrievability for large files.Proc.of CCS 2007, 584-597, 2007.
7. H. Shacham, and B. Waters, Compact proofs of retrievability. Proc. OfCryptology-ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.
8. G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphicidentification protocols. Proc. of ASIACRYPT 2009, 319-333, 2009.
9. A. F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensicsand Security, 10(3): 485–497, 2015.

AUTHOR PROFILE

Dr M Rama Bai, is working as Professor in Department of CSE at MGIT, Hyderabad, India. She has published more than 33 papers in international journals. Her research areas of interest include Image Processing, Machine Learning, Artificial Intelligence and Data Science.
Email: rama@mgit.ac.in

Maaz Bin Saad Quraishi, is currently pursuing M.Tech in Computer Networks and Information Security at MGIT, Hyderabad, India. His area of interest includes Threat Intelligence and Security Engineering.