ADVANCED INTRUSION DETECTION AND PROTECTION SYSTEM

Prashik Kamble[1], Bhushan Tikhe[2], Sachin Hande[3], Prof. Swapnaja Hiray[4]

Department of Comp. Engg, SKN Sinhgad Institute of Technology and Science, Lonavala, India [1 2 3 4]

prashikkamble.pnk54@gmail.com[1], bhushantikhe1@gmail.com[2], sachinhande40@gmail.com[3]

Abstract: The system proposes a security system, named the Internal Intrusion Detection and Protection System (IIDPS for short) at system call level, which creates personal profiles for users to keep track of their usage habits as the forensic features. The IIDPS uses a local computational grid to detect malicious behaviors in a real-time manner the proposed work is regarded with Digital forensics technique and intrusion detection mechanism. The number of hacking and intrusion incidents is increasing alarmingly each year as new technology rolls out. The system designed Intrusion Detection System (IDS) that implements predefined algorithms for identifying the attacks over a network. Therefore, in this project, a security system, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks at SC level by using data mining and forensic techniques. The system can identify user's forensic features by analyzing the corresponding SCs to enhance the accuracy of attack detection, and able to port the IIDPS to a parallel system to further shorten its detection response time.

Keywords: *Intrusion Detection Systems, Data mining, network, Vulnerable, Malicious, Authorization.*

I INTRODUCTION

In this digital age, computer and its subsidies have become so handy that all our day to day life is dependent on it. But due to increased chances of attacks we are asked for authentication at each and every step. We need to login into system or any application or any network, we require and need to successfully pass through authentication step. But in order to remember and store password, we have Human tendency to keep a simple or mostly a common password or pattern for every authentication purpose. This in turn increases the chances of intrusion. Security till date remains one of the biggest challenges and continuous efforts are taken to improve it. Still we face with large number of attacks such as DOS attack, phishing attack, eves dropping attack, spa email attack, Trojan horse attack, etc. All these attacks are easy to be detected at system call i.e. operating system level. Thus in this paper we are proposing a system that detect malicious harmful behavior basically called as Advance Intrusion Detection and Prevention System. Intrusion prevention monitors system structures for malicious activity or threat. It's a proactive approach which every organization should follow for safety and security purpose.

II LITERATURE REVIEW

[1] Analyzing log files for postmortem intrusion detection

Author: *K. A. Garcia, R. Monroy, L. A. Trejo, and C. MexPerera*

Description: Upon an intrusion, security staff must analyze the IT system that has been compromised, in order to determine how the attacker gained access to it, and what he did afterward. Usually, this analysis reveals that the attacker has run an exploit that takes advantage of system vulnerability. Pinpointing, in a given log file, the execution of one such an exploit, if any, is very valuable for computer security. This is both because it speeds up the process of gathering evidence of the intrusion, and because it helps taking measures to prevent a further intrusion, e.g., by building and applying an appropriate attack signature for intrusion detection system maintenance. This problem, which we call postmortem intrusion

Detection, is fairly complex, given both the overwhelming length of a standard log file, and the difficulty of identifying exactly where the intrusion has occurred. In this paper, we propose a novel approach for postmortem intrusion detection, which factors out repetitive behavior thus, speeding up the process of locating the execution of an exploit, if any. Central to our intrusion detection mechanism is a classifier, which separates abnormal behavior from normal one. This classifier is built upon a method that combines a hidden Markov model with k -means. Our experimental results establish that our method is able to spot the execution of an exploit, with a cumulative detection rate of over 90that speeds up the construction of a profile for ordinary system behavior.

[2] An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques

Author: *Fang-Yie Leu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao- Tung Yang*

Description: Currently, most computer systems use user IDs and passwords as the login patterns to authenticate users. How- ever, many people share their login patterns with coworkers and request these coworkers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviors launched from the outside world of the system only. In addition, some studies claimed that analyzing system calls (SCs) generated by commands can identify these commands, with which to accurately detect attacks, and attack patterns are the features of an attack Therefore, in this paper, a security system, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks at SC level by using data mining and forensic techniques. 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 his/her current computer usage behaviors with the patterns collected in the account holders personal profile. The experimental results demonstrate that the IIDPSs user identification accuracy is 94.29s, implying that it can prevent a protected system from insider attacks effectively and efficiently.

[3] Bio metric Authentication Using Mouse, Gesture Dynamics

Author: *Bassam Sayed, Issa Traore, Isaac Woungang, and Mohammad S. Obaidat*

Description: The mouse dynamics biometric is a behavioral biometric technology that extracts and analyzes the movement characteristics of the mouse input device when a computer user interacts with a graphical user interface for identification purposes. Most of the existing studies on mouse dynamics analysis have targeted primarily continuous authentication or user re-authentication for which promising results have been achieved. Static authentication (at login time) using mouse dynamics, however, appears to face some challenges due to the limited amount of data that can reasonably be captured during such a process. In this paper, we present a new mouse dynamics analysis framework that uses mouse gesture dynamics for static authentication. The captured gestures are analyzed using a learning vector quantization neural network classifier. We conduct an experimental evaluation of our framework with 39 users, in which we achieve a false acceptance ratio of 5.26 per and a false rejection ratio of 4.59.

[4] A Model-based Approach to Self-Protection in SCADA Systems

Author: *Qian Chen,Sherif Abdelwahed*

Description: Supervisory Control and Data Acquisition (SCADA) systems, which are widely used in monitoring and controlling critical infrastructure sectors, are highly vulnerable to cyber-attacks. Current security solutions can protect SCADA systems to monitor SCADA system performance, and proactively estimate upcoming attacks for a given system model of a physical infrastructure. We also present the feasibility of intrusion detection systems for known and unknown attack detection. A dynamic intrusion response system is designed to evaluate recommended responses, and appropriate responses are executed to attack impacts. We used a case study of a water storage tank to develop an attack that modifies Modbus messages transmitted between slaves and masters. Experimental results show that, with little or no human intervention, the proposed approach enhances the security of the SCADA system, reduces protection time delays, and maintains water storage tank performance. From known cyber assaults, but most solutions require human intervention. This paper applies autonomic computing technology.

[5] Detecting Web based DDoS Attack using Map Reduce operations in Cloud Computing Environment

Author: *Junho Choi, Chang Choi, Byeongkyu Ko, Dongjin Choi, and Pankoo Kim*

Description: A distributed denial of service attacks are the most serious factor among network security risks in cloud computing environment. This study proposes a method of integration between HTTP GET flooding among DDOS attacks and Map Reduce processing for 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.

III GAP IDENTIFICATION

Today in the age of computer and Smartphone's, it has become a tedious task for us to remember or Ids and passwords. Especially for working professionals where one needs to enter N numbers of user Ids and passwords, we start opting for a common pattern or password for every authentication. Thus it becomes easy for us to remember but as from security point of view, it becomes very easy and vulnerable for an attacker to attack a system or network. Intrusion basically refers to some outsider who does not belong to the group or community and is trying to intrude i.e. get into our system by wrong means. Thus intrusion detection basically refers to an act of detecting network system for malicious or harmful activity. It is an application which tries to identify and raise an alarm if any suspicious activity is tracked and observed. However here we are proposing a system which aims to identify internal intrusion in network or system. We are going to use data mining techniques to identify internal intruders and take action accordingly.

IV PROPOSED SYSTEM

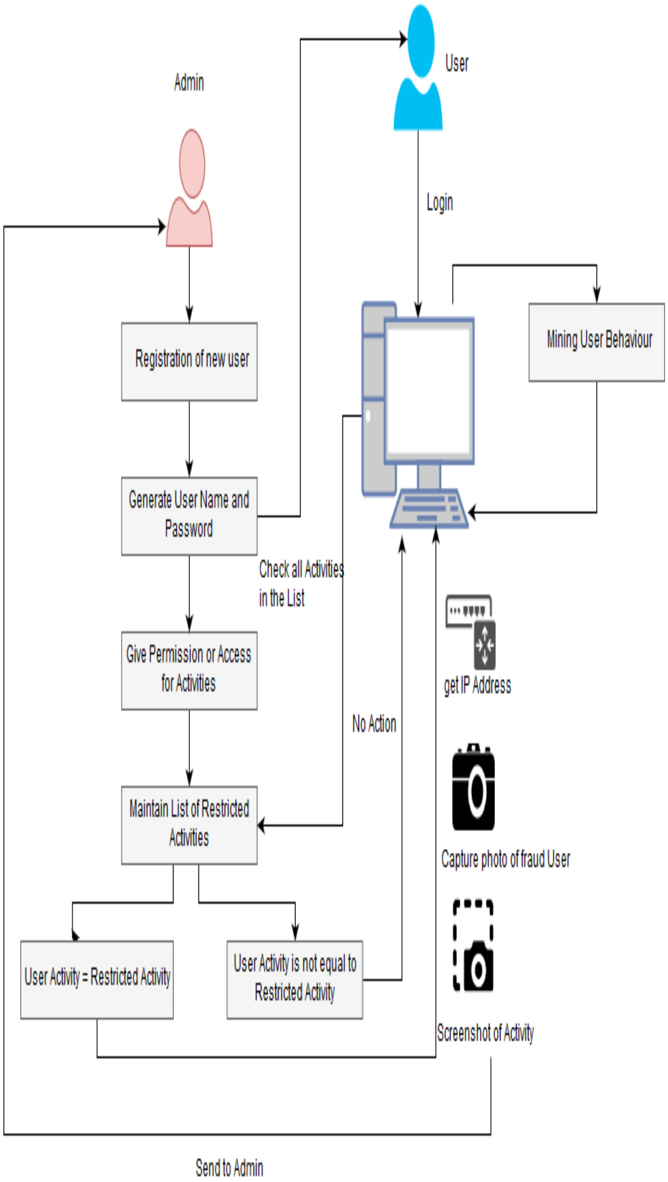
Admin
User
Login
Registration of new user
Mining User Behaviour
Generate User Name and Password
Check all Activities in the List
Give Permission or Access for Activities
get IP Address
No Action
Maintain List of Restricted Activities
Capture photo of fraud User
User Activity = Restricted Activity
User Activity is not equal to Restricted Activity
Screenshot of Activity
Send to Admin

Figure-1: System Design Architecture.

This proposed system aims at improving and providing high efficiency for intrusion detection. The analysis method monitors and provides details of routers, firewalls, packets, servers for detecting unauthorized entities. As we are using system calls to detect the intrusion attacks, this can be complimented using data mining and forensic techniques. It would help to identify and provide detailed information about a user and its SC patterns. IPS can be configured to monitor log and report activities. Here the duration of time is counted as it appears in the user's log file. After which the most commonly used SC patterns are filtered. These are then compared with user's daily habits and if any deviation is found then the reason for that needs to be identified. If the user has an exception on that particular instance than it can be ignored as a warning. But if no special particular instance is found then it needs to be alarmed and reported to the right authorities. Thus this would help in nay harmful after effect and prevent from any type of attacks. This helps to stop threat of attacks and is typically located between companies firewall and rest of network.

V CONCLUSION

We have successfully implemented an internal intrusion detection and preventions system. As the saying goes that prevention is better than cure, similarly we have aimed to build a system that prevents intrusion attacks and activities. This can be implemented from small scale to large corporate and non-technical areas as well. Also we have provided multiple modules and scenarios where we can keep a track and record of all the users and their activities. It will also help us generate trends which we can store in database and use it for future reference. It will also serve the purpose of maintaining logs which can be sent to higher and dedicated authorities for checking and preventing intrusion detections and harmful attacks or activities which do not have good intentions.

REFERENCES

[1] C. Yue and H. Wang, BogusBiter: A transparent protection against phishing attacks,ACM Trans. Int. Technol., vol. 10, no. 2, pp. 131, May 2010.

[2] 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. 110.

[3] H. Lu, B. Zhao, X.Wang, and J. Su, DifiSig: Resource dier- entiation based malware behavioral concise signature generation, Inf. Commun. Technol., vol. 7804,pp. 271284, 2013.

[4] Z. Shan, X.Wang, T. Chiueh, and X. Meng, Safe side eects commit- ment for OS-level virtualization, in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe,Germany, 2011, pp. 111120.

[5] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, Detecting web based DDoS attack using MapReduce operations in cloud computing environ- ment, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 2837, Nov. 2013.

[6] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer stream- ing, in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 15

[7] Z. A. Baig, Pattern recognition for detecting distributed node ex- haustion attacks in wireless sensor networks, Comput. Commun., vol. 34, no. 3, pp. 468484, Mar. 2011.

[8] H. S. Kang and S. R. Kim, A new logging-based IP traceback ap- proach using data mining techniques, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 7280,Nov. 2013.