An Intrusion Detection and Protection System for Securing Data with the Help of Data Mining and Forensic Techniques

[1]Balu Misal, [2]Prof.S.M. Shinde

Department of Computer and Science Engineering, SVERI's College of Engineering, Pandharpur.

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 a 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 and Protection System (IIDPS), System Call

I. INTRODUCTION

Intrusion detection systems (IDSs) sometimes defend against outside attacks. To evidence users, currently, most systems check user ID and word as a login pattern. However, attackers could install Trojans to filch victims' login patterns or issue an oversized scale of trials with the help of a lexicon to amass users' passwords. Once flourishing, they'll then log in to the system, access users' non-public files, or modify or destroy system settings. Fortuitously, most current host-based security systems and network-based IDSs can discover an acknowledged intrusion during a time period manner. However, it's terribly troublesome to spot WHO the aggressor is as a result of attack packets area unit usually issued with cast IPs or attackers could enter a system with valid login patterns. though OS-level system calls (SCs) are rather more useful in detection attackers and distinctive users, process an oversized volume of SCs, mining malicious behaviors from them, associate degreed distinctive attainable attackers for an intrusion area unit still engineering challenges. Security has been one of the serious problems in the computer domain since attackers very usually try to penetrate computer systems and behave maliciously to authenticate users. To solve this issue we propose a security system, named Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviors launched toward a system

II. EXISTING SYSTEM

In existing system, a model is proposed for such an attack based on network traffic flow. Specific network topology-based patterns are defined to model normal network traffic flow, and to facilitate differentiation between legitimate traffic packets and anomalous attack traffic packets. 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. Packet sniffer is not just a hacker's tool. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. When computers communicate over networks, they normally just listen to the traffic specifically for them. The disadvantage is that they cannot easily authenticate remote-login users and detect specific types of intrusions.

Disadvantages of existing system

1. It can be used for specific network topology-based patterns.
2. Detection accuracy is less.
3. Difficult to detect the malicious behaviors of users.
4. Tools used to detect malicious user which is not efficient technique.

III. PROPOSED SYSTEM

The proposed system provide a security system, named Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviors launched toward a system at SC level. The IIDPS uses data mining and forensic profiling techniques to mine system call patterns (SC patterns) defined as the longest system call sequence that has repeatedly appear several times in a user's log file for the user. The user's forensic features defined as an SC pattern frequently appearing in a user's submitted SC sequence but rarely being used by other users, are retrieved from the user's computer usage history. The system need to study the SCs generated and the SC-patterns produced by these commands so that the IIDPS can detect those malicious behaviors issued by them and then prevent the protected system from being attacked.

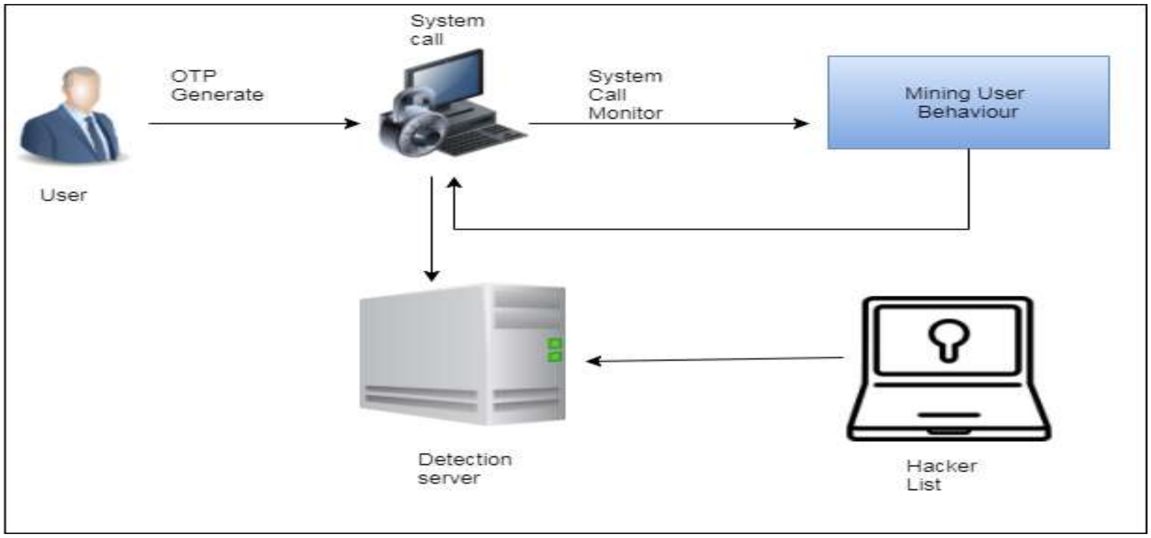


Fig: System Architecture

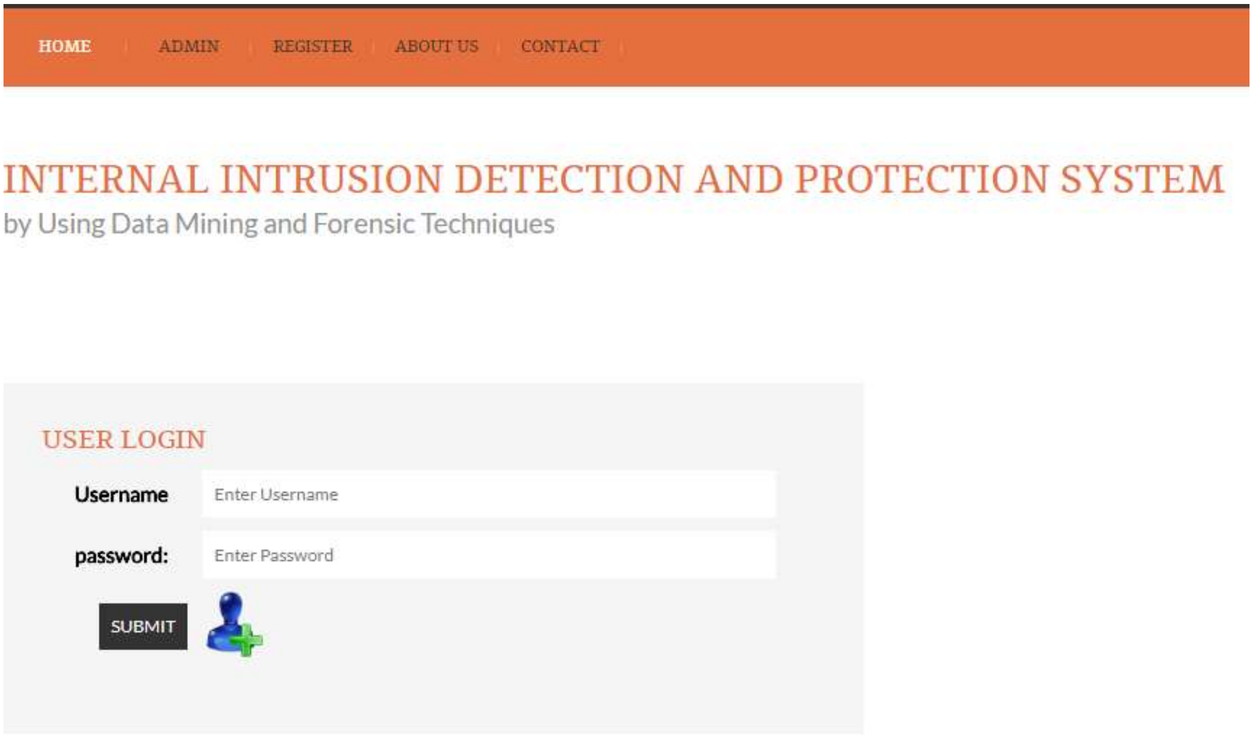
Advantages of Proposed System

1. Accuracy of detecting suspicious user is efficient than existing System.
2. Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviors of users.
3. Although other systems consume longer time for data analysis than the IIDPS does.
4. This can also detect malicious behaviors for systems employing GUI interfaces.

IV. CONCLUSION

The IIDPS (Internal Intrusion Detection and Protection System) employs data mining and forensic techniques to identify the user behavioral patterns for a user. The time that a habitual behavior pattern appears in the user's log file is counted, the most commonly used patterns are filtered out, and then a user's profile is established. By identifying a user's behavior patterns as his/her computer usage habits from the user's current input, the IIDPS resists suspected attackers. The future work of insider attack detection research will be about collecting the real data in order to study general solutions and models. It is hard to collect data from normal users in many different environments. It is especially hard to acquire real data from a masquerader or traitor while performing their malicious actions. Even if such data were available, it is more likely to be out of reach and controlled under the rules of evidence, rather than being a source of valuable information for research purposes.

V.RESULTS



INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM

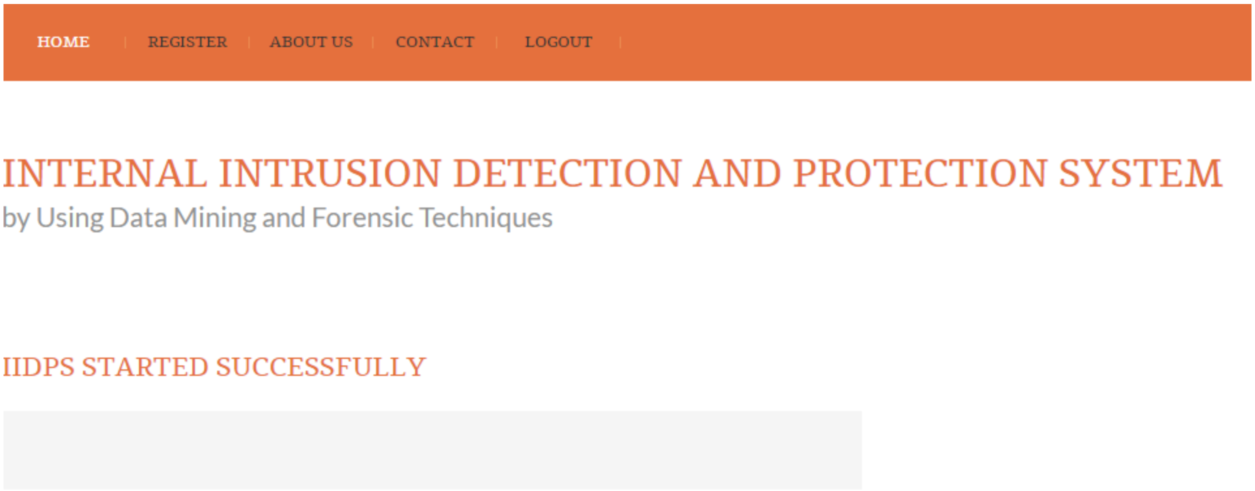
by Using Data Mining and Forensic Techniques

USER LOGIN

Username: Enter Username

password: Enter Password

Fig: Login Page



INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM

by Using Data Mining and Forensic Techniques

IIDPS STARTED SUCCESSFULLY

Fig: IDPS System started

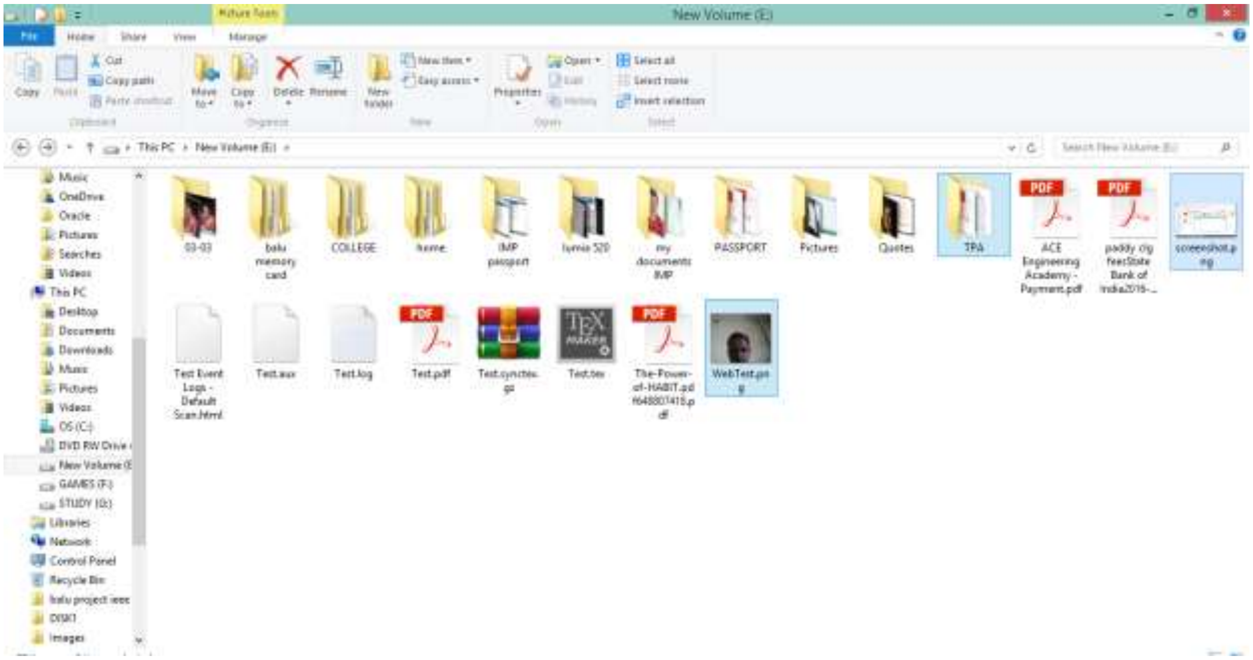


Fig: user attaching the pen drives to the system at that time also IIDPS takes the screenshot

REFERENCES

[1] 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.

[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. 1–10.

[3] H. Lu, B. Zhao, X. Wang, and J. Su, “DiffSig: Resource differentiation based malware behavioral concise signature generation,” Inf. Commun. Technol., vol. 7804, pp. 271–284, 2013.

[4] Z. Shan, X. Wang, T. Chiueh, and X. Meng, “Safe side effects commitment for OS-level virtualization,” in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120.

[5] 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.

[6] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, “MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming,” in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1–5.

[7] Z. A. Baig, “Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks,” Comput. Commun., vol. 34, no. 3, pp. 468–484, Mar. 2011.