IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 4, April 2017

# Providing Security and Internal Intrusion Detection to a system Using Forensic Techniques and Data Mining (IIDPS)

**Abhishek Chorage[1], Devashree Joshi[2], Aishwarya Bhatode[3], Mayuresh Devanpalli[4], M. K. Kodmelwar[5]**

Computer Dept, TSSM's BSCOER Narhe, Pune, India[1,2,3,4,5]

**Abstract:** As we know the computer systems use user IDs and passwords as the login patterns to authenticate users. So, many people share their login patterns with coworkers andrequest these coworkers to assist co-tasks, thereby making the pattern as one of theweakest points of computer security. The Insider attackers, the valid users of a system they attack the system internally, and so it's hard to detect since most intrusion detection systemsand firewalls identify and isolate malicious behaviors. Some studies also claimed that analyzing system calls (SCs) generated by commands can identify these commands, with which to accurately detectattacks, and attack patterns are the features of an attack. Hence, in this paper, named as the Internal Intrusion Detection and Protection System,it 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 astheir forensic features and determines whether a valid login user is the account holder ornot by comparing his/her current computer usage behaviors with the patterns collectedin the account holders personal pro le. The experimental results demonstrate that the IIDPSs user identification accuracy is 94.29 percentage, whereas the response time is less than 0.45s, implying that it can prevent a protected system from insider attacks effectively and efficiently.

**Keywords:** Data Mining, Internal Intrusion Detection and Protection System (IIDPS), SC level, forensic techniques.

## I. INTRODUCTION

As network-based computer systems plays an very important roles in society, they have become the targets of intruders. Therefore, there is a need to find the best possibleways to protect our systems.Security of a computersystem is an important factor. The security of a computersystem is compromised when an intrusion takes place. Defination of intrusion can be as any action done tohamper the integrity, confidentiality or availability of thesystem. There are some intrusion prevention techniqueswhich can be used to protect computer systems as a firstline of defense. But only intrusion prevention is not enough. Intrusion detection is required asanother measure to protect our computer systems from such type of vulnerabilities because As we know that systems become more complex, there are always exploitable weaknesses in the systems due to design and programming errors, or various penetration techniques.

Traditional intrusion prevention techniques, such as firewalls, access control and encryption, have failed to fully protect networks and systems from increasingly sophisticated attacks and malwares. As a result, intrusion detection systems (IDS) have become an indispensable component of security infrastructure used to detect these threats before they inflict widespread damage. While building an IDS we must consider many issues, like data pre-processing, intrusion recognition, data collection, reporting, and response. Among all of them, intrusion recognition is at the heart. Audit data are examined and compared with detection models, it describe the patterns of intrusive so that both successful and unsuccessful intrusion attempts can be identified.

Artificial intelligence and machine learning techniques were used to discover the underlying models from a set of training data. Commonly used methods were rule based induction, classification and data clustering. The automatically constructing models process from data is not trivial, especially for the intrusion detection problems. This is because intrusion detection faces such problems as huge network traffic volumes, highly imbalanced attack class distribution, the difficulty to realize decision boundaries between normal and abnormal behavior, and requiring continuous adaptation to a constantly changing environment. AI and machine learning have shown limitations to achieving high detection accuracy and fast processing times when confronted with these requirements.

In the past decades, computer systems have been widely employed to provide users with easier and more convenient lives. However, when people exploit powerful capabilities and processing power of computer systems, security has

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 4, April 2017

been one of the serious problems in the computer domain since attackers very usually try to penetrate computer systems and behave maliciously, e.g., stealing critical data of a company, making the systems out of work or even destroying the systems. Generally, among all well-known attacks such as pharming attack, distributed denial-of-service (DDoS), eavesdropping attack, and spear-phishing attack , insider attack is one of the most difficult ones to be detected because firewalls and intrusion detection systems (IDSs) usually defend against outside attacks. To authenticate users, currently, most systems check user ID and password as a login pattern.

However, attackers may install Trojans to pilfer victims' login patterns or issue a large scale of trials with the assistance of a dictionary to acquire users' passwords. When successful, they may then log in to the system, access users' private files, or modify or destroy system settings. Fortunately, most current host-based security systems and network-based IDSs can discover a known intrusion in a real-time manner. So, it is very hard to identify who is the attacker because attack packets are often issued with forged IPs or attackers may enter a system with valid login patterns. Although OS-level system calls (SCs) are much more helpful in detecting attackers and identifying users , processing a large volume of SCs, mining malicious behaviors from them, and identifying possible attackers for an intrusion are still engineering challenges.

Therefore, in this paper, The system propose 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 (SC-sequence) that has repeatedly appeared 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-sequences but rarely being used by other users, are retrieved from the user's computer usage history. The contributions of this paper are identify a user's forensic features by analyzing the corresponding SCs to enhance the accuracy of attack detection; able to port the IIDPS to a parallel system to further shorten its detection response time; and effectively resist insider attack.

In general, IDSs can be categorized two categories according to the detection methods they employ, namely (i) misuse detection and (ii) anomaly detection. Misuse detection identifies intrusions by matching observed data with pre-defined descriptions of intrusive behavior. So well-known intrusions can be detected efficiently with a very low false positive rate. For this reason, the approach is widely adopted in the majority of commercial systems.

## II. EXISTING SYSTEM

A model is proposed for such an attack based on network traffic flow. In addition, a distributed mechanism for detecting such attacks is also defined. 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.

## III. PROPOSED SYSTEM

The system propose a security system, named Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviors launched toward a system at SC level. In the IIDPS, the SCs collected in the class-limited-SC list, as a key component of the SC monitor and filter, are the SCs prohibited to be used by different groups/classes of users in the underlying system.

To verify the feasibility and accuracy of the IIDPS, three experiments were performed. The first defined the decisive rate threshold between the user profile established for u and each of other users' user profiles.The outcome extends the features, confirming that data mining and forensic techniques used for intrusion detection provide effective attack resistance. 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.

IJIREEICE

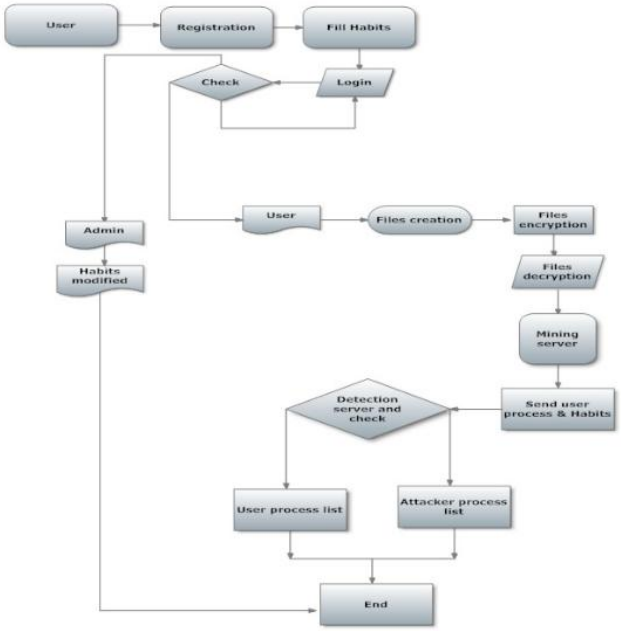
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 4, April 2017

## IV. SYSTEM ARCHITECTURE




## V. CONCLUSION

In this paper, an IIDPS is developed to detect insider attacks at SC level by using datamining and forensic techniques. The experimental results show that the IIDPS can effectively resist several aforementioned attacks. This process confirming that data miningand forensic techniques used for intrusion detection provide effective attack resistanceand also shows IIDPS may detect inaccurately when users habit suddenly changes. Nevertheless, in most cases, the IIDPS can still identify the legality of a login user. Whena user inputs a command, hundreds or thousands of SCs will be generated. Analyzinga huge number of SCs often takes a long time. The IIDPS spends 0.45 s to identify a user. Although other systems consume longer time for data analysis than the IIDPS does,how to mine SCs in an efficient method should be addressed. Employing a local computational grid can accelerate the processing speed of the miming server and detectionserver. A mathematical analysis on the IIDPSs behaviors is helpful in deriving its formalperformance and cost models, with which users can predict performance and cost of theIIDPS before using it. This can also detect malicious behaviors for systems employingGUI interfaces and then prevent the protected system from being attacked. The proposed model can be further used to increase detection accuracy and improve the decisive rate.

## REFERENCES

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, “Compartmented se-curity 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.
[5] 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.
[6] Z. Shan, X. Wang, T. Chiueh, and X. Meng, “Safe side effects commit-ment for OS-level virtualization,” inProc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120.
[7] M. K. Rogers and K. Seigfried, “The future of computer forensics: A needs analysis survey,” Comput. Security, vol. 23, no. 1, pp.12–16, Feb. 2004.
[8] 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.
[9] 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.
[10] Jonathon T. Giffin, Somesh Jha, and Barton P. Miller “Automated Discovery of Mimicry Attacks”, 2006.