Internal Intrusion Detection & Protection System using Data Mining & Forensic Technique

Sayyeda Zeba[1] Zarinabegam K Mundargi[2]
[1,2]SECAB Institute of Engineering & Technology, India

Abstract— Currently, most computer systems use user IDs and passwords as the login patterns to authenticate users. However, many people share their login patterns with co-workers and request these co-workers 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 behavior launched from the outside world of the system only. In addition, some studies claimed that analysing 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, 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 behaviours with the patterns collected in the account holder's personal profile. The experimental results demonstrate that the IIDPS's user identification accuracy is 94.29%, whereas the response time is less than 0.45 s, implying that it can prevent a protected system from insider attacks effectively and efficiently.

Key words: Intrusion Detection, Data Mining, Forensic Technique

I. Introduction

The computer systems are widely used to provide users with an easier and easier world. However, when people come across the powerful abilities and processing power of computer systems, since very usually attackers try to hack the computer systems and behave maliciously, e.g., critical data of a company is steeled , one of the serious problems in the computer domain is security systems are made out of work or even systems are also destroyed. Generally, from all the attacks such as distributed denial-of-service (DDoS), pharming attack, eavesdropping attack, and spear-phishing attack [1][2], insider attack is one of the most difficult attack to be detected because intrusion detection systems (IDSs) and firewalls usually excuse against outside attacks. Although, attackers have an option of installing Trojans to lift victims' login patterns or to encounter a large number of trials with the help of a dictionary in order to get the users' passwords. In order to authenticate the users, for now most of the systems check the pattern which is the login pattern using user ID and password .On successful attempt, attackers then may log in to the system ,in order to access private files of users, or to change or destroy the setting of the system. However, it is very difficult to know who the attacker is because attack packets are often attached with forged IPs or attackers can enter and use the system along with the valid login patterns. Happily most of current systems that are host-based security systems [3] and network-based IDSs [4], [5] can find a known trespass in a real-time manner. Even though OS-level system calls (SCs) are very much helpful in order to detect attackers and the identifying users [6], the engineering challenges include dealing with a large volume of SCs, extracting malicious activity from them, and then identifying all the possible attackers for an intrusion.

Currently, to keep safe the organization electronic assets, Intrusion Detection System (IDS) is critical requirement. To know whether the traffic is evil or not Intrusion detection is the process of knowing and analyzing the traffic on any device or network. That can be a software or physical appliance that checks the traffic which goes against organization security policies and all the standard security practices. In order to detect the intrusion and respond within time effective manner as a result chances of intrusions is devalued it continuously monitors the traffic. Host based Intrusion Detection System is arranged on a particular system/server. It continuously look after and analyze the activities of the system. On the basis of the deployment IDS broadly partitioned into two types i.e. Host based Intrusion Detection System (HIDS) and the other one is Network based Intrusion Detection System (NIDS). Tem where it is arranged.

II. Literature Survey

Computer forensics science, which views computer systems as crime scenes, aims to identify, preserve, recover, analyze, and present facts and opinions on information collected for a security event [7]. It analyzes what attackers have done such as spreading computer viruses, malwares, and malicious codes and conducting DDoS attacks [8]. Most intrusion detection techniques focus on how to find malicious network behaviour [9], [10] and acquire the characteristics of attack packets, i.e., attack patterns, based on the histories recorded in log files [11], [12]. Qadeer *et al.* [13] used self-developed packet sniffer to collect network packets with which to discriminate network attacks with the help of network states and packet distribution. O' Shaughnessy and Gray [14] acquired network intrusion and attack patterns from system log files.

These files contain traces of computer misuse. It means that, from synthetically generated log files, these traces or patterns of misuse can be more accurately reproduced. Wu and Banzhaf [15] overviewed research progress of applying methods of computational intelligence, including artificial neural networks, fuzzy systems, evolutionary computation, artificial immune systems, and swarm intelligence, to detect malicious behaviors. The authors systematically summarized and compared different intrusion detection methods, thus allowing us to clearly view those existing research challenges. These a fore mentioned techniques and applications truly contribute to network security.

However, they cannot easily authenticate remote-login users and detect specific types of intrusions, e.g., when an unauthorized user logs in to a system with a valid user ID and password. In our previous work [16], a security system, which collects forensic features for users at command level rather than at SC level, by invoking data mining and forensic techniques, was developed. Moreover, if attackers use many sessions to issue attacks, e.g., multistage attacks, or launch DDoS attacks, then it is not easy for that system to identify attack patterns. Hu *et al.* [17] presented an intelligent lightweight IDS that utilizes a forensic technique to profile user behaviors and a data mining technique to carry out cooperative attacks. The authors claimed that the system could detect intrusions effectively and efficiently in real time. However, they did not mention the SC filter. Giffin *et al.* [18] provided another example of integrating computer forensics with a knowledge-based system. The system adopts a predefined model, which, allowing SC-sequences to be normally executed, is employed by a detection system to restrict program execution to ensure the security of the protected system. This is helpful in detecting applications that issue a series of malicious SCs and identifying attack sequences having been collected in knowledge bases.

The Internal Intrusion Detection and Protection System, as shown in Fig. 1, consists of an SC monitor and filter, a mining server, a detection server, a local computational grid, and three repositories, including user log files, user profiles, and an attacker profile.

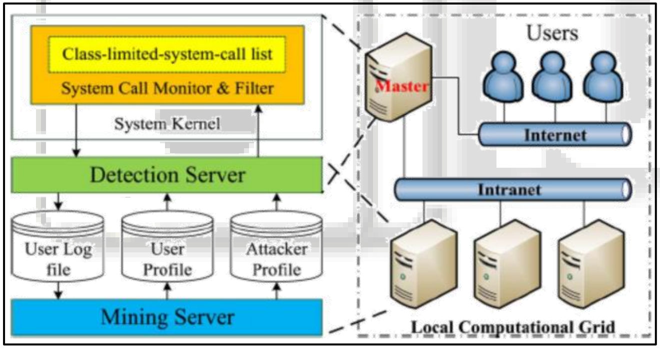

Fig. 1: System architecture

III. Results & Discussion

In this paper, an IIDPS is developed to detect insider attacks at SC level by using data mining and forensic techniques. The experimental results show that the IIDPS can effectively resist several aforementioned attacks. The outcome extends the features of [16], confirming that data mining and forensic techniques used for intrusion detection provide effective attack resistance. The second experiment indicates that the average detection accuracy is 94.29%. However, in Table VI, the accuracy of user backup is 89.97% since backup's log file has more common SCs than the other users'. It also shows that the IIDPS may detect inaccurately when user's habit suddenly changes. Nevertheless, in most cases, the IIDPS can still identify the legality of a login user.

IV. Conclusion

I have proposed an approach that employs data mining and forensic techniques to identify the representative SC-patterns for a user. The time that a habitual SC pattern appears in the user's log file is counted, the most commonly used SC-patterns are filtered out, and then a user's profile is established. By identifying a user's SC-patterns as his/her computer usage habits from the user's current input SCs, the IIDPS resists suspected attackers. The experimental results demonstrate that the average detection accuracy is higher than 94% when the decisive rate threshold is 0.9, indicating that the IIDPS can assist system administrators to point out an insider or an attacker in a closed environment. The further study will be done by improving IIDPS's performance and investigating third-party shell commands.

References

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security 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 commitment for OS-level virtualization," in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120. 3

[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. 1

[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. 6

[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. 2

[10] 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.

[11] 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.

[12] K. A. Garcia, R. Monroy, L. A. Trejo, and C. Mex-Perera, "Analyzing log files for postmortem intrusion

detection," IEEE Trans. Syst., Man, Cybern., Part C: Appl. Rev., vol. 42, no. 6, pp. 1690–1704, Nov. 2012.

[13] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in Proc. Int. Conf. Commun. Softw. Netw., Singapore, 2010, pp. 313–317.

[14] S. O'Shaughnessy and G. Gray, "Development and evaluation of a data set generator tool for generating synthetic log files containing computer attack signatures," Int. J. Ambient Comput. Intell., vol. 3, no. 2, pp. 64–76, Apr. 2011.

[15] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Comput., vol. 10, no. 1, pp. 1–35, Jan. 2010.

[16] F. Y. Leu, K.W. Hu, and F. C. Jiang "Intrusion detection and identification system using data mining and forensic techniques," Adv. Inf. Comput. Security, vol. 4752, pp. 137–152, 2007.

[17] Z. B. Hu, J. Su, and V. P. Shirochin "An intelligent lightweight intrusion detection system with forensics technique," in Proc. IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst.: Technol. Appl., Dortmund, Germany, 2007, pp. 647–651.

[18] J. T. Giffin, S. Jha, and B. P. Miller, "Automated discovery of mimicry attacks," Recent Adv. Intrusion Detection, vol. 4219, pp. 41–60, Sep. 2006.