ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Special Issue 5, March 2017

Efficient Intrusion Detection & Prevention System against Insider Attack by User Behaviour Mining

Gowtham C R[1], Anju.M[2], Jayashree.R[3]
Assistant Professor, Karpaga Vinayaga College of Engineering and Technology, Madurantakam [1]
UG Student , Karpaga Vinayaga College of Engineering and Technology, Madurantakam [2,3]

Abstract - In current modern world computer usage plays a vital role in human life. Most of the computer system use pattern systems to authenticate a valid user. However, many people share their login patterns with co- workers in-order to access their works. The user or the hacker who attacks the system internally is called as insider attackers. Insider attacker are the valid user of the system who are reasonable for the attacks. Therefore, here a security system is proposed to detect insider attacks at System Calls level by using data mining techniques. The security system creates user's personal profiles to keep track of user's routine activities. Whether a valid login user is the account holder or not by comparing his/her current computer usage behaviors with the patterns collect in the account holder's personal profile.

Index terms: *Network security, Insider attack, System call, Data mining.*

I. INTRODUCTION

In past computer systems have been widely Used for more convenient lives However when people access with the powerful capabilities and processing power computer systems suffer with the security issues such as insider attackers very usually try to penetrate computer systems and behave harmfully e.g., stealing critical data of a organization making the computer out of work or even destroying the systems. However, attackers may install Trojans to pilfer victims' when successful, they may then log in to the system, access users' private files, or modify or destroy system entirely. Mainly this method is used to prevent the application not the system [3] and network-based IDS [4], [5] can discover a known intrusion in a real-time manner. However, it is very complex to detect attacker packets are often issued with forged IPs or attackers may enter a system with valid login patterns. Although OS-level system calls (SC) are much more helpful in preventing attackers and [6], processing a large volume of SC, mining intrusion are still engineering challenges. The security system for computers and it is used to detect and protect internal intrusion.

II. MODULE DESCRIPTION

A. Mining User and Attacker habits

The behavior of user and attacker is analyzed here. Each user is identified with his unique Id and possesses a password for his profile. The behavior of each user can be viewed through his/her log files, work and search histories. Users have some specific access rights differentiating each user from others. Restricted actions and violation of access rights reveal a similar attack pattern which can be considered as an attacker habit.

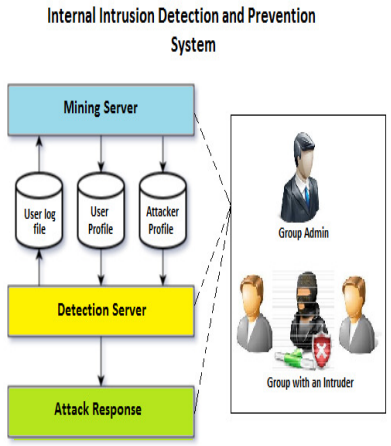

Figure 1: Intrusion detection and prevention system

B. User and Attacker Profile Generation

An unique profile which identifies a particular user is created for all users in the system. An attack pattern which may be an attacker specific pattern or a pattern commonly used by attackers is identified. With this identified attack pattern an attacker profile is created. All possible attacks to a system are included in the attacker profile.

C. Detection Server

User logs-in to his/her account and detection server keeps monitoring his/her actions. It keeps on comparing the profile of user with the attacker profile. If a match at any

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Special Issue 5, March 2017

instant of time is incurred, then the detection server sends an alert to the group admin to trigger the attack response to stop the attacker further intruding the system

D. Attack Response

Attack response is to prevent intruder from further snooping into the system. This responsive action is triggered by the group admin when the detection server finds an attack match. The user who is deploying an insider attack is tracked and logged out from his account.

E. Mining User and Attacker Habits

SC collected in *u*'s log file with a sliding window, named a log-sliding with, which is used to detect consecutive SC of size |Sliding window| along with their submitted sequence and partition the SC in the window into *k*-grams where *k* is the number of consecutive SC, *k* = 2, 3, 4, . . . ,|Sliding window| =10. In addition, another sliding window of the same size (i.e.,the same number of SC), called compared-sliding window(C-window for short), is employed to identify other SC-patterns also in *u*'s log file. This time, *k*' consecutive SC, preserving their submitted sequence, are extracted from a C-window to provide a total of (|Sliding window| − *k*_ + 1) *k*_ − grams, *k*_ = 2, 3, 4, . .|.The mining server invokes Algorithm, to match *k*-grams and *k*_-grams. At first, all SC collected in *u*'s log file are treated as a long SC-sequence. When all the _|Sliding window| *k*=2 (|Sliding window| − *k* + 1) *k*-grams ,derived from the L-window, have been compared with the_|Sliding window| *k*_=2 (|Sliding window|− *k*_ + 1) *k*_-grams, derived from the C-window, by using the longest common subsequence[22], which reveals the similarity between two strings by skipping noises, the C-window shifts right one input SC(e.g., originally beginning at position *x*, and then moves to the position beginning at *x* + 1),

III. Related Works

Computer forensic science, which seeks computer systems As crime scenes, aims to detect, 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 harmful codes, conducting security attacks [8]. Most intrusion detection Methods focus on how to find harmful network behaviors [9], [10] and acquire the characteristics of attack packets.

IV. Existing System

An Existing system's firewalls and intrusion detection systems usually defend against outside attacks such as pharming attack, distributed denial-of-service eaves dropping attack, and spear-phishing attack.

Insider attack is one of the difficult one to be detected. An existing host based and network based it can discover a known intrusion in a real time manner.

Also it is difficult to identify who the attacker is because attack packets are often issued with forged IP or attackers may enter a system with valid login patterns.

V. Proposed System

We propose a security system which detects malicious behaviors launched toward a system at System Calls. Our proposed system uses the data mining and the forensic profiling techniques to mine system call 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. It also stores the user inputs into the in the user's log file, which is a file keeping the SC submitted by the user following their submitted sequence. SC submitted by the user following their submitted sequence. The mining server checks and verify the log data with data mining techniques to identify the user's computer usage habits as user behavior patterns which are then recorded in the user's user profile. The detection server compares user's behavior patterns with those SC-patterns collected in the attacker profile and those in user profiles to respectively detect malicious behaviors and identify who the attacker is in real time. The advantages of this method are: It enhanced the accuracy of attack detection with the help of user's forensic features by analyzing the corresponding system calls. Shorten the detection response time and effectively resists insider attacks.

VI. Conclusion

Here we have proposed an approach that employs data mining and forensic techniques to identify the representative SC-patterns for a user. By identifying a user's SC-patterns as computer usage habits from the user's current input SC. The experimental results demonstrate that the average detection accuracy is higher than 95% when the decreasive rate threshold is 1.0, indicating that it can assist system administrators to point out an insider or an attacker.

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, "Bogus Biter: 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.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Special Issue 5, March 2017

[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.

[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 DDoSattack using MapReduce operations in cloud computing environment," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.