A Survey on Internal Intrusion Detection and Protection System Using Data Mining and Forensics Techniques

Ms. DIPALI VIJAY KARCHE, Prof. Mr.AMRIT PRIYDARSHI

[1] *PG Scholar,Departement of Computer Engineering Dattakala Faculty of Engineering,Pune Maharashtra,India*

Proffessor, *Departement of Computer Engineering Dattakala Faculty of Engineering,Pune Maharashtra,India*

Abstrct: ***There are different ways to protect the data as well as the networks from attackers. Firewalls are used to protect passwords as per need. Many times these are not enough. Due to that systems and networks are always under the observation of thread. Intrusion detection system(IDS) detects unwanted activities of computer system, which are comes through the internet. The manipulation may take form of attacks by hackers. But it is observed that most firewalls and IDS commonly try to protect computer system against outsider attacks. This paper focuses survey on different data mining and forensic techniques to detect and protect internal computer system from intrusion using Internal Intrusion Detection and protection system Using Data Mining and Forensic Techniques(IIDPS) to find out insider attacks at SC level with the help of Data mining and Forensic Technique.***

***Key words*: Functionality ,Identify user, tf-idf, user log file, Attacker profile.**

I INTRODUCTION

Today everyone access the network based information .So via networks many attackers enter into system. These attacks are not only outsider but also insider . In outsider attacks the unauthorized users get access to the systems by using different types of attacks In case of insider attacks the authorized users try to compromise the integrity, confidentiality or availability of resources. Intrusion means any set of activities that try to harm the security goals of the information. Various approaches like as encryption, firewalls, virtual private network, etc., But they were not enough to secure the network fully.

Hence, Internal Intrusion Detection and Protection System (IIDPS), is used as security tools in this system to creates users' personal profiles to keep track of users' regular habits as their forensic features and determines whether a authorised login of user or not and if not then comparing users current computer usage behaviours with the patterns collected in the user's personal profile. Internal Intrusion Detection and Protection System (IIDPS), which detects behaviours at SC level. The IIDPS uses data mining and forensic profiling techniques to mine system call patterns that has repeatedly appeared several times in a user's personal profile. According to user's forensic features, defined as an SC-pattern frequently appearing in a user's submitted habits , but rarely being used by other users, are find out from the user's computer usage history.

II EXISTING SYSTEM

Several information security techniques are available today to protect information systems against unauthorized use, duplication, alteration, destruction and virus attacks.

Firewall:

The main purpose of a firewall is to prevent unauthorised access between networks. that means protecting a sites inner network from internet. But disadvantage of firewall is that a firewall looks outwardly for intrusion in order to stop them from happening. Firewall limits access between networks to prevent intrusion and do not signal an attack from inside network.

Network based IDS:

A Network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of services attacks,port scans or even attempts to cracks into computers by monitoring network traffic.Some network based IDSs have problem dealing with network based attacks that involve fragmenting packets,These malformed packets causes the IDSs to become unstable and crash.

Host based IDS:

Host based IDSs monitor all or parts of the dynamic behaviour and analyzes the internals of computing system rather than on its external interfaces.The principle of operation of HIDS depends on the fact that successful intruders or crackers will generally leave a trace of their activities ,such as keystroke logging, identify theft spamming, botnetactivity, spyware-usage etc.

Host based IDS are harder to manage , as information must be configured and managed for every host mentioned and not suited for detecting network scans or other such surveillance that target an entire network ,because the IDSs only sees those network packets received by its host.

Intrusion Detection and Protection System (IDPS):

Intrusion detection and Protection system detects systems effected activities and also normal activities to secure information. But it is very difficult to find out large volume o.s system calls and different behaviour and identify attackers of an intrusion.

Comparison between existing system and IIDPS

By studying this paper three types of attacksobserved, Type-I attack in which users group members are not allowed to submit system calls. While in Type-II attack generates sensitive system call which modify settings or data, and last third Type-III, it successfully enter into security system.

Table I indicates comparison of existing system with IIDPS with respect to attack type and identify valid user function, Where 'N' symbol indicates system doesnot provide mentioned function and 'Y' indicates provide designated function.

Table I Comparative analysis of the Existing systems & IIDPS

Existing systems	Attack type			
OSSEC	Identify user	Type – I	Type -II	Type -III
AIDE	N	Y	Y	N
SAMHAIN	N	Y	Y	N
SYMANTE CSP	N	Y	Y	N
IIDPS	N	Y	Y	Not completely
OSSEC	Y	Y	Y	Y

Table II shows difference between response time of IIDPS system with other system detecting attacks n identify user

Existing systems	Response time(Seconds)			
OSSEC	Identify user	Type – I	Type – II	Type III
AIDE	N	60	60	N
SAMHAIN	N	60	60	N
SYMANTE CSP	N	60	60	N
IIDPS	N	2	2	3
OSSEC	0.45	0.001	0.001	0.45

III An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques

This paper gives features like as,

- Find out users habit by using forensic techniques.
- Use data mining techniques to check out repeatedly occurred system calls from user behaviour profile.
- Protect system from insider attack.

SYSTEM FRAMEWORK

System Frame work has major components, Detection server , Mining Server, Local computational grid and system call monitor and filter and also have three repository systems such as user log file, user profile ,attacker profile.

SC Monitor and Filter:

System call monitor and filter collects system call from system kernel which is in the form of user id, process id and system call.System call s are nothing but the bridge between user applications and services provided by kernel.

In execution of simple commands number of system calls generated hence its needed to filter that system calls which are repeatedly used.To find out which type system call generated ,static model named as frequency-inverse document frequency (TF-IDF) is used.

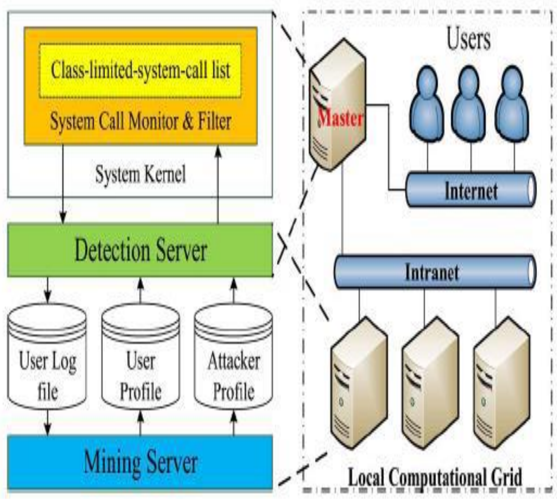

Figure. IIDPS system framework

Mining Server

With the help of data mining techniques mining server find out users habits which are stored in user profile. After that compare this user habit with all other users habit to identify malicious behaviour of attacker. In this process two steps are involved

- Mining User and Attacker Habits
- Creating User Profiles and Attacker Profile

Detection Server

Detection server compare attacker profile with user profile which showsmalicious behaviour.If there is intrusion detected then it notify to the SC monitor and filter to isolate the user from the protected system to prevent user from continuously attack.

Computational Grid

Detection server and the mining server are run on the local computational grid to support the IIDPS's onlinedetection and mining speeds and increase its detection and mining capability. The computational grid is nothing but the collection of internally connected computers working together as a single integrated computing resource.

ADVANGENTS

- IIDPS system provide comprehensive protection against identity theft, information mining, and network hacking
- Constant Network Monitoring while user asleep or away from computer.
- The IIDPS system is able, to monitor both the outside attacks and patterns of behaviour which may be detected within the system.
- The main disadvantage of intrusion detection systems is their inability to tell friend from foe, is overcome using IIDPS system.
- Techniques used for intrusion detection provide effective attack resistance.
- Average detection accuracy is higher.

APPLICATIONS

- A credit card company to identify customers most likely to be interested in a new credit product.
- Health Record Management

IV CONCLUSION

This paper focuses on survey of techniques for data mining and forensic to internal intrusion detection and protection.IIDPS system enables data mining and forensic technique to identify system call , creating user profile and isolated from attacker profile to protect user from internal attack.

REFERENCES

[1]Fang-YieLeu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao-Tung Yang,'' An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques",IEEE Int. Conf. Avail., Rel. Security, Taiwan,pp 1932-8184,2015

[2] 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.

[3] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Syst. J.*, vol. 7, no. 2,pp. 262–274, Jun. 2013.

[4] S. C. Arseni, E. C. Popovici, L. A. Stancu, O. G. Guta, and S. V. Halunga,"Securing an alerting subsystem for a keystroke-based user identification system," in *Proc. Int. Conf. Commun.*, Bucharest, Romania, 2014,pp. 1–4.

[4] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-streambased intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *IEEE Syst. J.*, vol. 9, no. 1, pp. 1–14, Jan. 2014.

[5] 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.

[6] 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.

[7] S. Yu, K. Sood, and Y. Xiang, "An effective and feasible traceback scheme in mobile internet environment," *IEEE Commun.Lett.*, vol. 18, no. 11,pp. 1911–1914, Nov. 2014.

[8] AIDE. [Online]. Available: http://aide.sourceforge.net/

[9] SAMHAIN. [Online]. Available: http://www.la-samhna.de/samhain/

[10] Symantec CSP. [Online]. Available: http://www.symantec.com/criticalsystem-protection.