ISSN 2395-1621

Implementation of Internal Intrusion Detection and Protection System Using Data Mining

[#1]Mahendra Badole, [#2]Suhas Bhalerao, [#3]Milind Kamble, [#4]Anmol Shinde,
[#5]Prof. Reshma Patil

[#1234]Department of Computer Engineering,
[#5]Assistant Professor, Department of Computer Engineering

K. J College of Engineering and Management Research Pune.

ABSTRACT

There are different ways to protect the data as well as the networks from attackers. As per need Firewalls are used to protect passwords. 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.

ARTICLE INFO

Article History

Received: 14th May 2018

Received in revised form :

14th May 2018

Accepted: 16th May 2018

Published online :

21st May 2018

Keywords: Functionality, Identify user, user log file, Attacker profile.

I. INTRODUCTION

Today all over world access the network based information. So via networks many attackers enter into system. We assume that attacker is only outsider but these can be insider. Unauthorized users get access to the systems in outsider attacks by using different types of attacks. Authorized users try to compromise In insider attacks. 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 authorized login of user or not and if not then comparing users current computer usage behaviors with the patterns collected in the user's personal profile. Internal Intrusion Detection and Protection System (IIDPS), which detects behaviors at SC level. The IIDPS uses data mining and forensic profiling techniques to mine system call patterns that have repeatedly appeared several times in a user's personal profile. As per the forensic features, defined as an user's submitted habits appearing frequently in a System Call-pattern but other users rarely being used are find out from the user's computer usage history.

II. MOTIVATION

Moto of developing this system is to protect systme from insider or who known to credential of system.and find out or detects the malecious activity in system launched toward a system using this system.

III. EXISTING SYSTEM

In 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, speeds up the process of locating the execution of an exploit, if any. Classifier is central to our intrusion detection mechanism, which classify/separates abnormal behavior of intruder. 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 traffic analysis, troubleshooting, network traffic monitoring, and other most important purposes. When computer/system communicate over networks, they normally just listen to the traffic specifically for them.

In 1980, the concept of intrusion detection began with Anderson's seminal paper; the existing system introduced a threat classification model that develops a security monitoring surveillance system based on detecting anomalies in user behavior. In 2003, Kaining Lu Zehua Chen Zhigang Jin JichangGuo, has presented one collaborate IDS module to make a real-time detection and block intrusions before occurrences based on HIDS using sequences of system call anomaly detection. In 2009, ChunhuaGu and Xueqin Zhang, proposed a system using rough set for attribution reduction and support vector machine for intrusion detection classification. In 2009,

Yong-Xiang, Xia Zhi-Cai Shi and Zhi-Hua Hu, proposed a method of detecting intrusion using incremental SVM based on key feature selection. Again in the same year, Rung Ching Chen, Kai-Fan Cheng and Chia-Fen Hsieh, used RST (Rough Set Theory) and SVM (Support Vector Machine) to detect intrusions. RST is used to reprocess the data and reduce the dimensions. Next, the features were selected by RST will be sent to SVM model to learn and test respectively. In 2010 with the Support Vector Machines (SVMs) Eid effectively introduced intrusion detection system by using Principal Component Analysis (PCA). In2011, Shingo Mau, Member, IEEE, has described a novel fuzzy class-association rule mining method based on genetic network programming (GNP) for detecting network intrusions. Once more same year, Jie Zhang and Carol J Fung have proposed to measure the level of trust among IDSes according to their mutual experience using Dirichlet-based trust management. Recently in 2012, has described an adaptive network intrusion detection system which uses a two stage architecture. To detect potential anomalies in the traffic is the first stage a probabilistic classifier. In the second stage a HMM based traffic model issued to narrow down the potential attack IP addresses.

Disadvantages:

- They cannot easily authenticate remote-login users and detect specific types of intrusions.
- They did not mention the SC filter.
- A secretary cannot submit some specific privileged SCs.
- It cannot represent any one of the four commands.
- Sequential parts cannot be executed in parallel.

IV. PROPOSED SYSTEM IMPLEMENTATION

In proposed system, the system proposed for protect to the system, named Internal Intrusion Detection and Protection System (IIDPS), which detects/identify malignant/ unlegitimate activity happen in a system . The outcome extends the features, confirming that data mining and forensic techniques used for intrusion detection provide effective attack resistance.

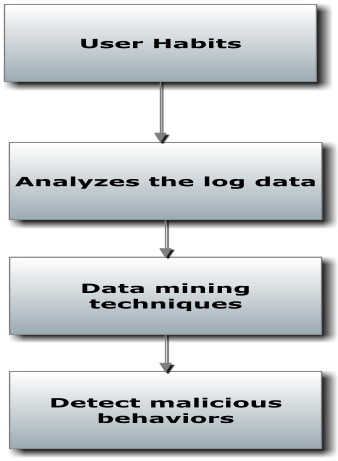
MODULES:

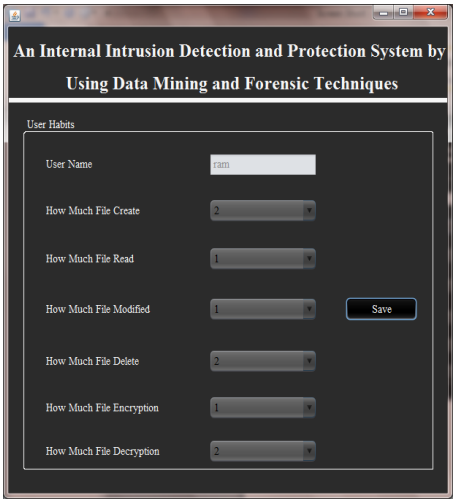
- User habits
- Mining Server
- Detection Server
- Attackers

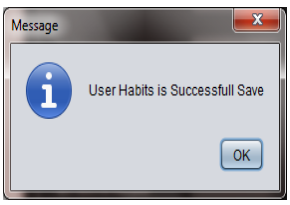
MODULE DESCRIPTION

User Habits:

The mining server analyzes the log data with data mining techniques to identify the user's computer usage habits as his/her behavior patterns, which are then recorded in the user's user profile. The detection server compares users' behavior patterns with those SC-patterns collected in the attacker profile, called attack patterns, and those in user profiles to respectively detect malicious behaviors and identify who the attacker is in real time. When an intrusion is discovered, the detection server notifies the SC monitor and filter to isolate the user from the protected system. The purpose is to prevent him/her from continuously attacking the system.

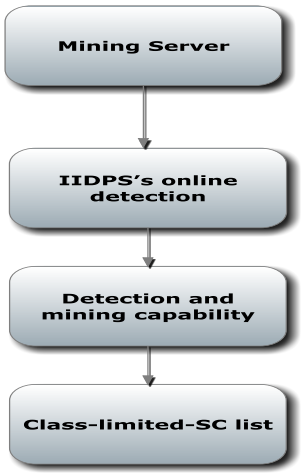


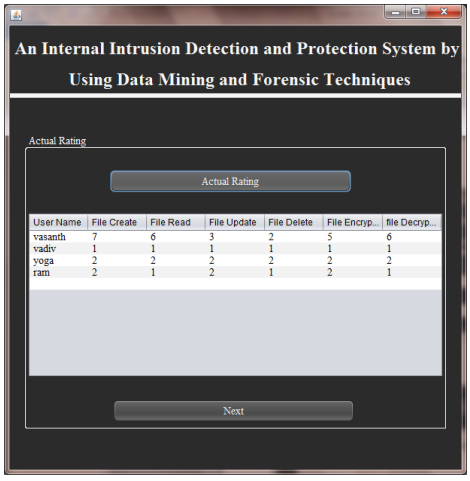


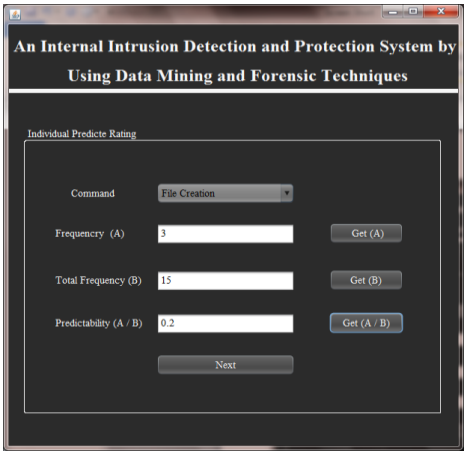


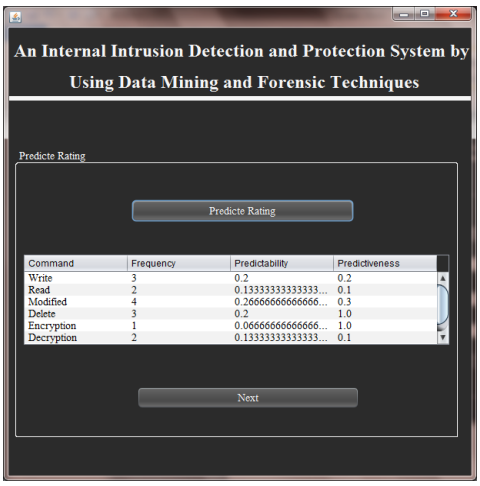
Mining Server:

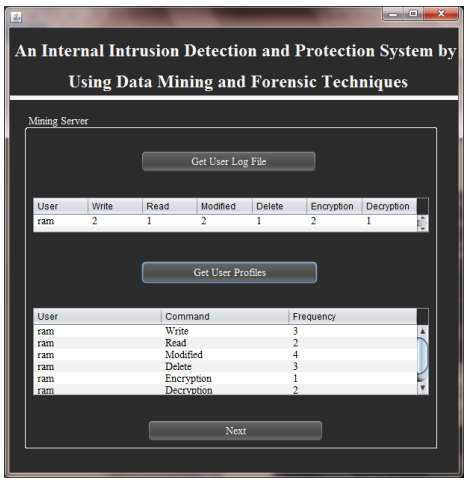
Both the detection server and the mining server are run on the local computational grid to accelerate the IIDPS's online detection and mining speeds and enhance its detection and mining capability. If a user logs in to the system by using another person's login pattern, the IIDPS identifies who the underlying user is by computing the similarity scores between the user's current inputs, i.e., SCs, and the behavior patterns stored in different users' user profiles.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.







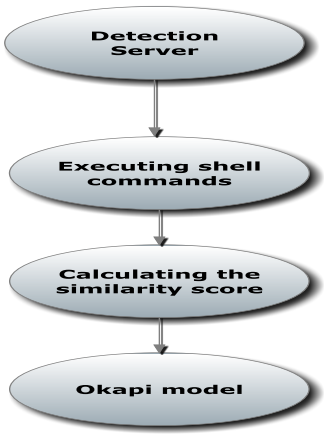


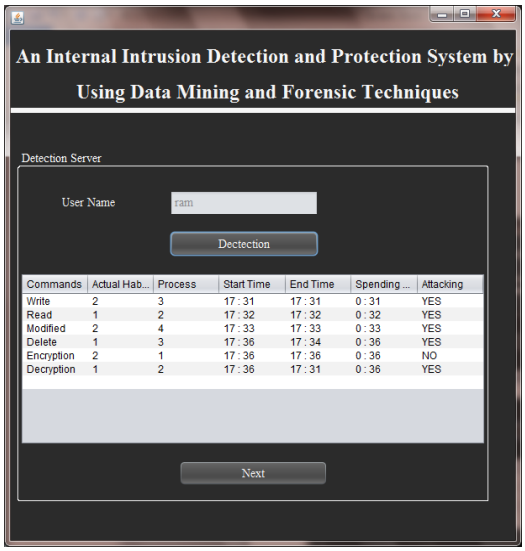


Detection Server:

The detection server captures the SCs sent to the kernel by the underlying user u when u is executing shell commands and stores the SCs in the u 's log file. Now sever tries to calculating the similarity score between the user is account holder or not by calculating similarity score using newly generated SCs denoted by NSCu, in the u 's current inputs and the usage habits, i.e., forensic signatures, stored in u 's user profile to verify u . The Okapi model, which is utilized to calculate the similarity score between user j 's user profile Uhj and an unknown user u 's current input SC-sequence, denoted bySim (u,j) , is defined as

$$Sim(u,j) = \sum_{i=1}^{p} F_{iu} \cdot W_{ij}$$





Attackers:

An attack pattern, which may be an attacker-specific pattern or a pattern commonly used by attackers, can be identified in the same method. Similarly, an attack pattern that an attacker frequently submits but others have seldom or never submitted will be considered as one of the attacker's representative attack patterns and will obtain a high similarity weight. Hence, signatures collected in an attacker profile can be classified into common signatures and attacker-specific signatures. The latter can be used to identify who the possible attackers are when a protected system is attacked by attacker-specific signatures.

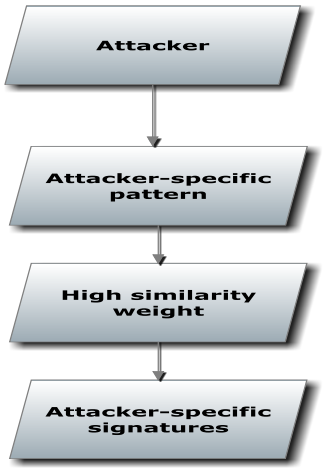


Fig:- System Framework

Email Security option

In previous paper system detect only insider attack but now when attacker attack on the system, system generate the mail and automatically send to the main user of the system so we can check illegal activity and claim on the attacker. Email contains the **INTRUDER IP ADDRESS AND HOST NAME.**

Advantages:

1. It identifies a user's forensic features by analysing the corresponding SCs to enhance the accuracy of attack detection.
2. It able to port the IIDPS to a parallel system to further shorten its detection response time.
3. It effectively resists insider attack.
4. The IIDPS can detect those malicious behaviours issued by them and then prevent the protected system from being attacked.
5. The mining user profiles by using an unsupervised cluster approach can also improve the performance of the mining process.
6. When insider attacked on system or illegal activity done, system send mail to the main user of system.

APPLICATIONS

1. System can be used in college.
2. System also used in organizations.
3. System also useful in the cyber cafes.
4. System also used for the personal use.

Mathematical model:

System Description:
Let W is the Whole System Consists:
U is the set of number users. U=U1,U2Un.
S:is the IIDS which detects the internal malicious activities of user.
UA:is set of user activates. UA=ua1, ua2, ua3, . . . uan.
A:be set of attack i.e. malicious activities of user.
A=a1,a2, . . .an.
D:be the detection server which detects the malicious activities of user from which id detected
in A.

1. U be the user login to the system .
U = fU1, U2g
U1=U11,U12 .....U1n.ADMIN
U2=U21,U22.....U2n.Normal User

2. U1 is set of activities that is admin that define the habit for Normal user.
S = C, D, U, E, D, R
C=Create
D=delete
U=update
E=Encryption
D=Decryption
R=Rename

3. A be set of attack i.e. malicious activities of user.
A = C, D, U, E, D, R
C=Create
D=delete
U=update
E=Encryption
D=Decryption
R=Rename

4. D: be the detection server which detects the malicious activities of user from which id detected in A. if Normal user or Attacker do any changes in system then it detect.

V. LITERATURE SURVEY

Literature Survey			
year	Title of Paper	Author	Description
2015	A study of secured Design of smart meter with Energy Efficient in Smart grid	M.AsanNainar, G.Dharani Devi	This paper describes A smart grid is the integration of information and communications technology into electric transmission and distribution networks.
2014	Autonomous Fault Detection In Self-Healing Systems using Restricted Boltzmann Machines	Chris Schneider Adam Barker Simon Dobson	The system present a novel methodology for autonomously generating investigation leads that help identify systems faults, and extends our previous work in this area by leveraging Restricted Boltz- mann Machines (RBMs) and contrastive divergence learning to analyse changesin historical feature data.
2011	Safe Side Effects Commitment for OS-Level Virtualization	Zhiyong ShanXin Wang Tzi-cker Chiueh	In this work, we develop a VM commitment system called Secom to automatically eliminate malicious state changes when merging the contents of an OS-level VM to the host
2010	The use of computational intelligence in intrusion detection systems	Shelly Xiaonan Wu, Wolfgang Banzhaf	The research contributions in each field are systematically summarized and com- pared, allowing us to clearly define existing research challenges, and to high- light promising new research directions. The findings of this review should provide useful insights in to the current IDS literature and be a good source for anyone who is interested in the application of CI approaches to IDSs or related fields.
2010	A Model based Approach to Self-Protection in SCADA Systems	Qian Chen Sherif Ab-delwahed	This paper applies autonomic computing technology to monitor SCADA sys- tem performance, and proactively estimate upcoming attacks for a given system model of a physical infrastructure.

Difference between existing system and proposed system

Sr. No	**Existing System**	**Proposed System**
1	Unable able to provide security at SC level	Provide Security at SC level
2	Not able to provide e-mail based system alert	Provide e-email based security alert
3	Unable to detect an Internal Intrusion	Able to detect an internal Intrusion
4	Encryption and Decryption of data files are not provide	Encryption and Decryption of data files is provide
5	Only External Intrusion detect	Internal and External Intrusion can detect

VI. FUTURE WORK

This system can be used to detect the host intrusion detection where host machine comprises the confidential files.
Attackers can attack on host machine that attacks would be detect by the system and updated files can be recovered by System. This system can detect the files modification and also prevent the file modification. If files deleted from the Host machine permanently then system can recovered the files.

VII. CONCLUSION

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. This process confirming that data mining and forensic techniques used for intrusion detection provide effective attack resistance and also shows 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. When a user inputs a command, hundreds or thousands of SCs will be generated. Analyzing a huge number of SCs often takes a long time. The IIDPS identify a user. Although other systems consume longer time for data analysis than the IIDPS does, This GUI interfaces and then prevents the protected system from being attacked. The proposed model can be further used to increase detection accuracy and improve the decisive rate.

REFRENCES

[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, Some sh Jha, and Barton P. Miller "Automated Discovery of Mimicry Attacks", 2006.

