Improving Accuracy in Decision Making for Detecting Intruders

Monika Sehgal[#1], Nitin Umesh[#2]

Department of Computer Science, Lovely Professional University
Phagwara (Punjab) India

***Abstract*—** Normal host based Intrusion detection system provides us some alerts of data integrity breach on the basis of policy violation and unauthorized access. There are some factors responsible if any employee of the enterprise access some files on which basis policy and permissions are applied. If these are incorrectly applied then false positive rate of intrusion detection increases. To minimize this rate and to better understand about the user who access unauthorized file, a framework is proposed which assemble data and information from diverse devices, and a special active record will be created, which will help the administrator to take better decision which will improve accuracy in decision making and more supportive policies and permissions can be implemented on intrusion detection system. This will also improve the storage system's performance by less recovery operations.

***Keywords*—** Storage system, Policy, Database, Intrusion detection, Permission, Security.

I. INTRODUCTION

As the data is increasing day by day in an enterprise and number of user access data from one storage system also increases. So the Database or Storage security is very major issue and it need protection from all the users who are accessing it even from inside organization. Because authorized users can also misuse the database and try to access the data for which they are not authorized and user can also try to change the data file or directory and can harm the integrity of the data. Intrusion detection systems are used in such case. Host based intrusion detection system operate on a specific host and monitor the activities. It checks policy violation, unauthorized access and maintains data integrity. Network based intrusion detection system operate on network segments checks the network traffic and monitor multiple host, perform packet analysis and detect attacks. Intrusion detection detect according to different methods, In Anomaly based detection network activity is determined like bandwidth used by the system, and provide alert when find something unusual happens. In Signature based detection few patters are already stored and these patterns are taken from attacks already happen and detected which help to find out if same kind of attack happens. In Application based detection authorized user are checked if they are exceeding their authorization and transaction logs are checked. In Policy based or Rule based parameters like access permission given to user and applied to files and other set of rules are checked.

As the size of organization increases managing policies becomes more tedious and error prone. To avoid the security breaches and network vulnerability, the analysis of these policies are required.[1] Even though there are so many detection and prevention systems to protect our system from attacks and intrusion, still many attacks happen every day, like unauthorized login, document sniffing and authorized files are under the threat of access and cracking. Single Host based IDS cannot provide all the functionality. A survey of 182 IT security and operational professionals departments are focused on gaining visibility into their applications and processes for managing security policies. Under 'Greatest challenge when it comes to managing security device in organization' Lack of visibility into network security policies is 21.7 %. Under 'Greatest risk enterprise faces today' Lack of visibility into application is 28.7% and insider threats are 27.5%. So this survey reveal internal security management is big requirement and it is very important do work on insider threats and managing policies.[11], [12].

Inside Threat is when a malicious person who is an employee of enterprise or company tries to access the file and data for which he/she is not authorized. We easily notice the outside organization security vulnerability, we some time ignore inside security vulnerability. Employees can theft the company information. Some steps should be taken to secure the data from inside threats. By applying passwords, access policies to secure the documents and files and limiting access, but these can also be violated. A single Host based IDS cannot provide all the functionality. So suitable approach need to combine several security techniques, intrusion detection with information integration. A mechanism is proposed which create a report of all the users those are accessing the storage. Whenever any change is detected in system like someone try to access or modify the file or directory for which he is not permitted or authorized, and rule violation will occur a report is generated and email is send to the authorized person to give him a report. And report will also contain the information that what changes have occur. One daily report is created which will keep track of all the information of users. Even the user is not performing any vulnerable task, and no doubt this report will also contain the information of intruder and what activity he/she perform on the system, and a final report of all the activities of suspicious user is created

by differentiating from the report of all the users accessing data or files. This report will be analysed by the administrator who analyse the report and take decision that the violation was actually malicious or fair. On the decision of the admin policy can be updated. This will further improve the security of data storage.

A. *Terminology used in intrusion detection*

Few alarms are generated from intruder detectors while checking and analysis. These alarms are as follows:

- False Positive: This tells the alert is generated by the IDS but there was no threat and attack was actually performed. So this misleads host system.
- True Positive: This tells the alert is generated by the IDS when there was threat and attack was actually performed.
- False Negative: This tells the alert is not generated produced by the IDS but there was actual attack or threat happens. So this avoid the intruder or vulnerable activity.
- True Negative: This tells the alert is not generated by the IDS there was no threat and attack was actually performed [6].

II. Related Work

There are lots of security tools and techniques and research is going on for network based intrusion detection, but for host based intrusion detection very few work is going o because we think that existing tools are enough and provided us full security at host level which we require.

Carol J Fung, Member, Jie Zhang and Raouf Boutaba has proposed a Distributed host based IDS collaboration system that maintain acquaintance list, of other host to collaborate and share the information about intrusion. Different user can have different signature and information of intrusion. Bayesian learning technique helps to expert Host IDS with past experience of other nodes. This helps to evaluate their false positive and false negative rate. This will help new user for better intrusion detection and this is done to enhance the accuracy of intrusion detection [1].

Surachai CHITPINITYON, Kasom KOHT-ARSA, Surasak SANGUANPONG, Jatuporn CHUCHUAY proposed a Policy based Network Access Control Framework. Framework set a communication between distinct devices which is control by Policy and Configuration Manager. NAC help for checking and granting permission. Detector detect traffic anomaly events and report to PCM. By analysis if alert message match with policy new configuration or rules are created and send to PE [2].

Khalid Alsubhi, Issam Aib, Jerome Francois and Raouf Boutaba proposed a Policy based Framework for configuration and control of security enhancement mechanisms. Dynamic policy based adaption mechanism is used between the Snort signature-based IDPS and light weight anomaly based FireCollaborator IDS. Security measures based on assessment of system vulnerability and threat prediction provides several level of attack containment. A report is generated on the risk that are likely to threat the information in near future [3].

Amel Meddeb-Makhlouf, Yacine Djemaiel, Noureddine Boudriga proposed a Multi level IDS is collaborate through Global intrusion Detection and tolerance architecture. It collect the data from different network components and correlate them and detect the distributed attacks at their early stages. Scalability problem and fault tolerance vulnerability and unable to detect attack targeting storage is solved by Global detection and global correlation and intrusion tolerance integration. It allow the tolerance and detection of complex attacks from information gathered by components located locally and remotely[4].

Mohammad Banikazemi, Dan Poff, Bulent Abali, Thomas J. Watson perform the intrusion detection on the storage system. Two prototypes are used. First is performing real time intrusion detection inside a storage management system. This system is IBM TotalStorage SAN Volume Controller (SVC). In this system file based Id access rules are converted into block based rules. Second is deploying intrusion detection system and loosely coupled it with SAN, no internal modification on the storage system is required in this method. If any changes occur on new copy old copy will replace new corrupted copy, and this process occurs at after few minutes[5].

III. Proposed Architecture

Proposed architecture consists of parts: A. Setting policies and configuration. B. Violation fetching. C. Information collection and aggregation. D. Filtering and correlation. E. Analysis and policy update.

A. *Setting Policy and Configuration*

First of all files, folders and directories security policies and permissions are applied and configuration files are implemented by administrator of database or storage system. And new rules are created according to those policies. These rules are like:

1) Insert permission on file F1 by E1 group.
2) Delete permission on file F2 by A1 group.
3) Insert permission on file F1, F2, F3 by M1 group.
4) Delete permission on file F1, F2 by M1 group.
5) Update permission on file F1, F2 by M1 group.

B. *Violation Fetching*

On the basis of policy, permissions and access rules applied if any changes and modification on file and directories are monitored and data integrity is breaches.

The information about which file was accessed and changed is recorded. This can be done by the intrusion detection tools. These tools are Host based IDS like Tripwire[9], OSSEC[10]. These tools match the previous file's hash with new file's hash to find any changes done over it or not. Then the information of suspicious person accessing the data, either harming our data storage system or not will be captured and a report of each employee or group is generated differently. This report format is like:

1) Group M1 Update the file F3.
2) Group E1 Insert the file F2.

TABLE I
FULL REPORT FORMAT AFTER COLLECTION AGGREGATION

Transaction ID	Event ID	File	Command	Group	Creation Time	Modification time	IP Address
TS 1	EV 12	F3	Update	M1	11-Jan-2012 PM 12:18:24	11-Jan-2012 PM 12:25:54	172.19.2.12
TS 2	EV 23	F2	Insert	E1	13-Jan-2012 PM 15:53:45	13-Jan-2012 PM 16:02:15	192.17.3.1
TS 3	EV 27	F2	Insert	A1	16-Jan-2012 AM 11:42:56	16-Jan-2012 PM 12:03:25	172.168.1.2
TS 4	EV 38	F3	Delete	M1	17-Jan-2012 PM 17:14:45	17-Jan-2012 PM 17:15:46	192.19.12.4

3) Group A1 Insert the file F2.
4) Group M1 Delete the file F3.

C. *Information Collection and Aggregation*

All the possible information of suspicious person(can be intruder or not depend on administrator's final decision) is collected from diverse devices and report of suspicious person or employee is created differently, which will contain all the historical and current data about that user like Transaction ID, Event ID, Which file was accessed, Permission misused, Creation timing, Modification timing, IP address of that person. New full report created shown in Table. 1.

D. *Filtering and Correlation*

Finally first report which was created by intrusion detection tools and policies defined by admin and the new full report which was created by collection of information from diverse devices are correlated and new final record to detect the suspicious employee is intruder or not is fetched and filtered by admin. This information is fetching by keep in mind few cases and looking from reports that which file was accessed before accessing and changing unauthorized file. Few cases are mentioned here which can cause false alarms and which are required to noticed before filtration.

In large organizations some time employee's roles and group changed but in records permissions are not fully changed so it shows violation and shows unauthorized access even after employee is accessing authorized file. Second case is sometimes after accessing one file access of another file is very urgent but for that permission is by mistake not given so it shows violation. Another case is if two departments has same course file and one department has access file of that same course, but other department has applied a rule that no other department can access their files. So these cases required some information which is provided after this step of correlation and filtering. This is shown by Fig. 2.

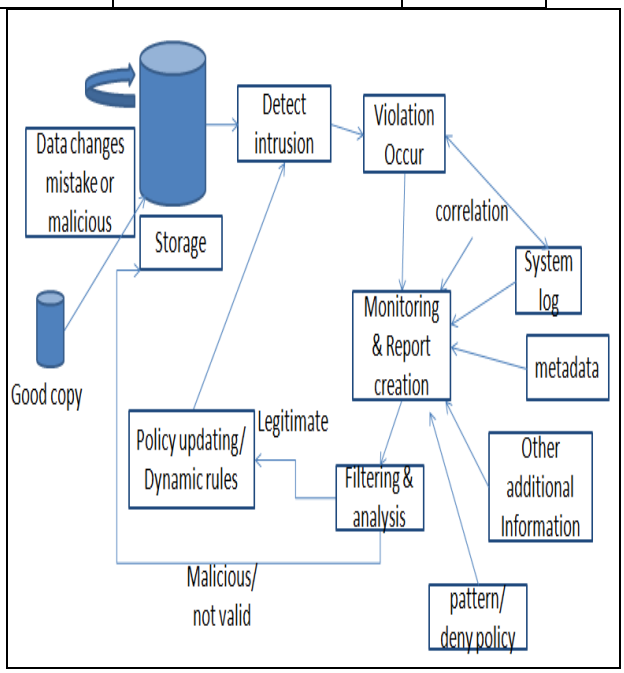

Fig. 1 Model of Proposed Architecture.

E. *Analysis and Policy Update*

According to rules violation alerts and operation performed and authentication provided intruder is filtered in better way by admin. This filtered report provides better and refined information about suspicious person, which is analysed by the database or storage administrator. If the suspicious person is not an intruder then policy and configuration files are updated and no updation of storage from good or old copy is performed. And if suspicious person is

intruder then more restriction is applied to particular employee and group.

In this way accuracy of detecting intruder is improved by admin. At last according to new report and decision taken by the admin, policy file is updated and new rules formation done.

If employee is not intruder according to final report then no updation of storage is done or less recovery is done on storage system and database then we can evaluate performance of host or storage server will be far better because no time will be lost, and processing time to do the task also saved and very less overhead will be due to reduction of extra updation and recovery from old database.

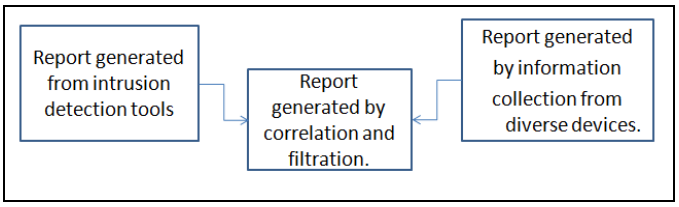

Fig. 2 Report after Filtering and Correlation.

IV. Conclusions

A report is created by aggregating information of suspicious person from diverse devices. This will help the administrator of organization to detect whether the intruder is actually intruder or this is false alarm. Hence from report False positive rate will decrease and fewer false alarms will generate which also help to make less updation of database from the original or good copy and increase the performance of storage or host terminal.

References

[1] Carol J Fung, Jie Zhang and Raouf Boutaba, "Effective Acquaintance Management based on Bayesian Learning for Distributed Intrusion Detection Networks" , IEEE, 2012.

[2] Surachai CHITPINITYON, Kasom KOHT-ARSA, Surasak SANGUANPONG and Jatuporn CHUCHUAY, "Design and Implementation of Open Framework for Policy-Based Network Access Control", IEEE,2009.

[3] Khalid Alsubhi, Issam Aib, Jerome Francois and Raouf Boutaba, "Policy-Based Security Configuration Management Application to Intrusion Detection and Prevention", IEEE, 2009.

[4] Amel Meddeb-Makhlouf, Yacine Djemaiel and Noureddine Boudriga, "Cooperating systems for Global Intrusion Detection and Tolerance", IEEE, 2007.

[5] Mohammad Banikazemi, Dan Poff and Bulent Abali, "Storage-Based Intrusion Detection for Storage Area Networks (SANs)" Proc. of the 22nd IEEE / 13th NASA Goddard Conference on Mass Storage Systems and Technologies (MSST'05), IEEE.

[6] Difan Zhang, Wei Yu and Rommie Hardy, "A Distributed Network-Sensor Based Intrusion Detection Framework in Enterprise Networks" IEEE, 2011.

[7] Hazem Hamed and Ehab Al-Shaer, "Taxonomy of Conflicts in Network Security Policies", DePaul University, 2006 IEEE.

[8] Sarwar Alam "Network Security And Intrusion Detection System" Department of Computer Science and Engineering, BRAC University, Dhaka, Bangladesh, (2007).

[9] http://www.tripwire.org

[10] http://www.ossec.net

[11] http://www.darkreading.com/insider-threat/167801100/security/security-management/232900252/biggest-threats-come-from-inside-the-enterprise-survey-says.html.

[12] The State of Network Security: Attitudes and Opinions AlgoSec Survey Insights (2012).