7th International Conference & Exposition on Petroleum Geophysics

"HYDERABAD 2008"

P - 304

The semi-automated Intrusion Detection System for Secure Information Management

Mr. Ananta Kumar Biswas,

Senior Programming Officer, SPIC, ONGC, Panvel, Mumbai, anantab10@yahoo.com

Summary

Like oil and gas reserves, information is one of organization's most vital resources. Whether this data is used upstream for exploration and production activities, or downstream for refining and distribution, data is crucial to operations. In today's marketplace, reliable access to information- from geophysical to drilling, from transport to refining- is important in obtaining maximum value from assets and is key of sustaining global competitive advantage. As a solution of securing data intrusion detection system is used to better manage data and information workflow. These Intrusion Detection Systems detect attacks by capturing and analyzing network packets. In this paper Semi-automated Intrusion Detection System is proposed which is a new way to identify intrusion characteristics. The key techniques used here are sensing audit and syslog data analysis, generating response, database management, and generating report. The functional components are logging host and IDS server. The logging host is used for sensing log data, generating local response, and sending sensed records to IDS server and the IDS server is used for generating global response and report based on query given by system administrator.

Introduction

Today's oil and gas companies are facing many challenges, including:

- Exponential data growth and terabyte-sized project data sets are placing intense pressure on the petrotechnical computing environment and forcing companies to take a new look at how growing volumes of data should be managed and protected.
- High costs as reservoir data is unused for periods of time. The expense of managing historical volumes continues to increase.
- Aligning business needs and technology expenditures to ensure the appropriate level of performance, protection, and availability to support business unit application requirements.
- Protecting data from planned and unplanned outages, and accidental or malicious detection.

Intrusion Detection Systems are software or hardware products that automate this monitoring and analysis process. Intrusion detection allows organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. There are several compelling reasons to acquire and use Intrusion Detection Systems:

- To detect attacks and other security violations those are not prevented by other security measures.
- To document the existing threat to an organization.
- To act as quality control for security design and administration, especially of large and complex enterprises.
- To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.

Intrusion detection systems perform the following functions well:

- Monitoring and analysis of system events and user behaviors
- Recognizing patterns of system events that correspond to known attacks
- Recognizing patterns of activity that statistically vary from normal activity

- Managing operating system audit and logging mechanisms and the data they generate
- Alerting appropriate staff by appropriate means when attacks are detected.

There are four fundamental functions of IDS: Monitoring, Analysis, Response, and Generating Reports as shown in Figure 1. The different sources of event information can be drawn from different levels of the system, with network, host, and application monitoring system.

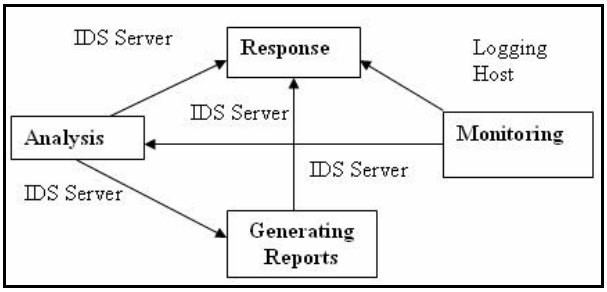

Figure 1: Functions of IDS

In this paper the proposed Semi-automated Intrusion Detection system can monitor, analyze, store logging information from multiple sources, generate alarms and on the basis of stored information can generate report for future study of intrusion characteristics by System Administrator to take proper action against intruder. So by this semi-automated process, attack launched during periods of high traffic could be found out. The security is more in case of this type of analyzer because of its isolation from outside network. This not only is more effective in protecting network infrastructure but also helps to recover more previously compromised hosts. It is likely to be a more effective deterrent against further intrusion attempts because of manual investigation by administrators in offline.

Theory and Method of Intrusion Detection

The security policies for industry are:

- Protection of data: Measures are in place to ensure network and data security
- Use of data: Use of client data is strictly for the purpose of serving the client objective
- Return of data: The client controls their data and has right to request its return at any time

A. Architecture

Each logging host acts as an intrusion sensor to sense system log and also as a network sensor to perform real-time traffic analysis and packet logging on IP networks. The IDS server acts as an analyzer, report and response generator with the help of system administrator as shown in Figure 2. The active intrusion detection is done by host sensor and the offline analysis is done in server with the help of administrative console. Administrative console is used to analyze the detected information stored in database by making queries to the server.

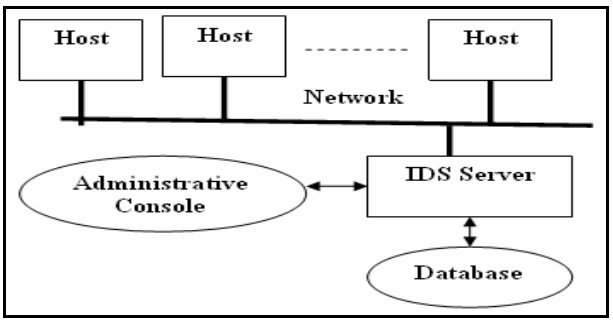

Figure 2. Secure Semi-automated Intrusion Sensing and Analysis System

B. Description of Functional Components

The proposed technique has been designed with the following functional components: Logging host, IDS Server. The interactions among these functional components are shown in Figure 3. The multiple logging hosts sense the intrusion from different system and audit log files as well as sense the network using lightweight intrusion detection tool to perform real-time traffic analysis and packet logging on IP networks. They generate one local response in real time when intrusion is detected and send the sensed data to the IDS server which is connected in the same LAN. The logging host and IDS server communicate through one ephemeral port specified in IDS client server program. The IDS server is totally isolated from outside user intervention as the all well known ports of IDS server are blocked, so it is self secured. In IDS server the received data is stored in one standard format. The data stored in the database with the help of manual interaction by the system administrator can be further analyzed. On the basis of intrusion characteristics report and global response are generated for future protection.

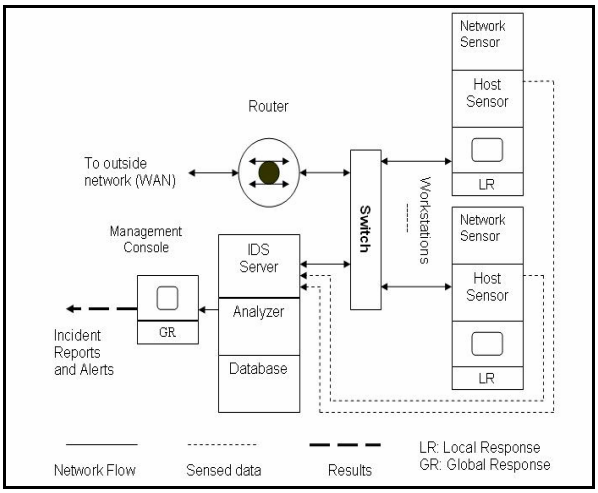

Figure 3. Design of the proposed Intrusion Sensor and Analyzer

C. Features

The confidentiality of intrusion information is maintained by authentication as the authentication information is changed periodically. The availability of the hosts in network is satisfied by detecting and preventing the intrusion by the manual intervention of the system administrators. The integrity of the intrusion information is never lost due to continuous monitoring of host sensor and generating alarms after intrusion detection. The security of the IDS server is maintained by blocking all well known ports only some ephemeral ports will be open through which the logging hosts can communicate. No outsider intervention can be possible. The most interesting feature of the proposed system is the semi-automation. Due to high network traffic sometimes intrusions are missed and sometimes false detection can be happened in online. These two phenomena are called miss intrusion detection and false positive. These can be removed by manual intervention of system administrator in offline. This offline analysis is done in IDS server. The main features of the proposed technique are shown in Figure 4.

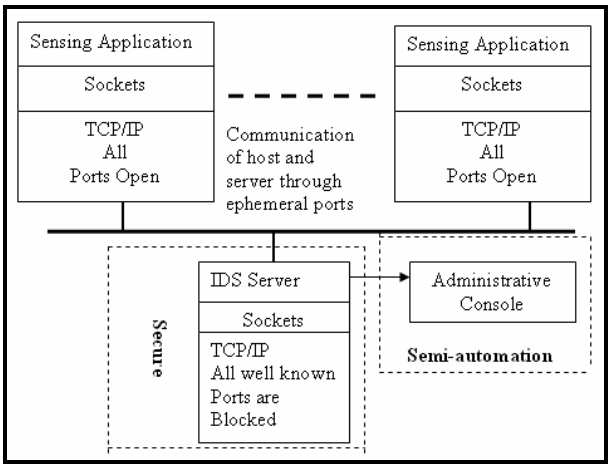

Figure 4. Semi-automation and security in proposed Technique

D. Implementation Procedure

The logging host is implemented in UNIX system by using the sensing program to sense the intrusion from syslog and audit log data files [11]. The syslog.conf file is configured in such a way that all the specific debugging messages will be stored in the specified log file as shown below:

/etc/syslog.conf:
auth.debug /tmp/auth.log
mail.debug /tmp/mail.log
daemon.debug /tmp/daemon.log
*.debug @remote-host

Command to start snort
./snort -l ./log -h 10.205.134.0 -c snort.conf

Rules stored in rules /local. rules

alert tcp $HOME_NET any -> $HOME_NET 21 (msg:"ftp intruder";content:"passwd";)
alert tcp $HOME_NET 23 -> $HOME_NET any (msg:"telnet intruder"; content:"passwd";)

Alert logged by Snort

08/24-13:48:15.409968 [**] [1:0:0] ftp intruder [**] [Priority: 0] {TCP} 10.205.134.102:32807 -> 10.205.134.101:21

08/24-13:53:50.960606 [**] [1:0:0] ftp intruder [**] [Priority: 0] {TCP} 10.205.134.102:32809 -> 10.205.134.101:21

After detection of intrusion in the system the pop up alert messages are generated using the developed sensing program. The snort tool is used to detect network intrusion

and alert messages are generated. The client server communication is made through normal client server program. In the server side the detected information is stored in database. The administrator interacts through administrative interface by sending queries and reports are generated. Based on that report the administrator takes the proper preventive action.

Existing Techniques

The following gives a brief description about some case studies:

(1) Security Agility Response to Intrusion Detection is designed with the help of Common Intrusion Detection Framework (CIDF) [1] and the Intrusion Detection Working Group (IDWG) ([2], [3]) of the Internet Engineering Task Force (IETF). The architectural goals are carried out by three primary elements: an agile policy, an Agility Authority (AGA), and an agility subsystem. Together, these elements also provide much of the infrastructure to support the intrusion response capabilities. This paper has presented a strategy to generate automated host-based responses to intrusions by combining security agility with cooperative frameworks for intrusion detection and response. Though this technique is automated but there is no manual intervention for further analysis which can lead to generate the basic problem of IDS such as false positives, miss intrusion detection incident etc. No active network based intrusion detection [9] concept is used.

(2) In a distributed autonomous-agent network-intrusion detection and response system each agent operates cooperatively yet independently of the others, providing for efficiency, real-time response and also providing significant advantages in scalability, flexibility, extensibility, fault tolerance, and resistance to compromise. The proposed scheme notifies other agents [10] on other computers in a network of attacks so they can take preemptive or reactive measures. A neural network is designed to measure and determine alert threshold values. A communication protocol is proposed to relay these alerts throughout the network. The agents are processes that run on each host, monitoring that host for intrusive activity and communicating with each other in a coordinated response to this activity [5]. But here the host agents are not secured as they are not isolated from outside intervention and there is no future analysis on the collected data and no network wide correlation is used.

(3) Tracing Based Active Intrusion Response (TBAIR) is a new way to address the problem of network-based intrusion based on Sleepy Watermark Tracing (SWT). TBAIR [6] is able to effectively trace the detected intrusion that utilizes stepping stone to disguise its origin at real-time, and dynamically push the intrusion countermeasures such as remote monitoring, blocking, containment and isolation. Through SWT's unique active watermark technique, TBAIR is able to trace even when the intrusion connection is idle. It is more active response paradigm to help to better repel or eliminate network-based intrusions and have identified the need of effective network-wide intrusion source tracing in order to build automated, network-wide response system. It is the better approach over the IDIP (Intrusion Detection and Isolation protocol) [4] that uses an active approach to trace the incoming path and source of intrusion using boundary controllers collaboratively locate and block the intruder by exchanging intrusion detection information, namely, attack descriptions. Therefore IDIP requires each boundary controller to have the same intrusion detection capability as the IDS at the intrusion target host. The active network [7] is an emerging framework that seeks to increase the programmability of computer networks and network components. This trust model is appropriate for tracing but may not be fit for active intrusion response as a compromised router could do

Intrusion Detection and Analysis System				
Security Agility Response to Intrusion Detection	*Distributed autonomous-agent network-intrusion detection and response system*	*Tracing Based Active Intrusion Response*	*Self securing storage technique*	*Semi-automated Intrusion Detection System*
Advantage: host based automated response	Advantage: network based detection and response manual control	Advantage : active network based intrusion detection network wide tracing	Advantage: offline diagnosis manual control, more secure, active network based intrusion detection	Advantage: Active network based intrusion detection offline analysis no overhead to the host IDS server is more secure as it is isolated from outsider intervention Server is able to generate response no chance of miss detection, false positives etc.
Disadvantage: No active network based detection no manual control problem of miss detection, false positives etc.	Disadvantage: host agents' information is not secured as it is not isolated from outside intervention There is no future analysis on the collected data Overhead to every host	Disadvantage: no manual control IDS is not secured no offline diagnosis overhead to every host	Disadvantage: overhead to host no response from self securing storage	No such disadvantage on the basis of existing mechanism

Table 1. Comparison

much more during active intrusion response than just tracing. No security is added here so that the IDS will be totally isolated from outside world: it can sense the intrusion but nobody will be able to hear its presence. Also no offline diagnosis is done here by system administrators.

(4) Self-securing storage technique takes an active part of an intrusion survival strategy [8]. From behind a thin storage interface (e.g., SCSI or CIFS), a self-securing storage server can watch storage requests, keep a record of all storage activity, and prevent compromised clients from destroying stored data. It describes three ways self securing storage enhances an administrator's ability to detect, diagnose, and recover from client system intrusions. Combined, these features can improve an organization's ability to survive successful digital intrusions i.e., it is helping to more quickly detect intrusions, providing easily accessible information for diagnosing intrusions, and simplifying and speeding up post-intrusion recovery. But here this self-storage server can't generate any report and response.

The comparison between the proposed technique and existing techniques is based on the host based and network based active intrusion detection, network wide tracing, availability and confidentiality of host sensor and IDS server, less overhead to host sensor, local response generation by host sensor, offline analysis in IDS server, administrator intervention (semi automation), offline global response generation, report generation, making standard formatted database, database management in server, and reduction of miss intrusion incidents, false positive. Many of the existing approaches didn't consider any offline diagnosis and security of the IDS server which are advantages of the proposed technique. The comparison is shown in TABLE I.

Conclusion

Confidentiality and security of data is of importance in outsourcing so this semi-automated intrusion detection system is a step in maintaining the confidentiality of data and have a high security set-up to protect data. Semi-automated intrusion detection system with the features confidentiality, integrity, availability, security, and manual control has been designed and implemented. The logging host is designed and implemented by developing the sensing program collecting data from log files, and generating local response in real time. The sensed data is sent to the IDS server for further analysis and to store it in database so that the data can be queried by the system administrator to generate report and alert in offline. Security is provided by the isolation of IDS server from the outsider intervention by blocking the ports and semi-automation is provided with the interaction of system administrator so that miss intrusion detection, false positives etc can be eliminated. This technique is one of the active network based intrusion detection and analysis system as it can generate alert also in offline.

References

[1] P. Porras, D. Schnackenberg, S. Staniford-Chen, M. Stillman, and F. Wu. "The Common Intrusion Detection Framework," CIDF working group document, http://www.gidos.org.

[2] H. Debar, M.-Y. Huang and D. Donahoo. "Intrusion Detection Exchange Format Data Model," Internet Draft, Internet Engineering Task Force, January 2000.

[3] R. Feiertag, C. Kahn, P. Porras, D. Schnackenberg, S. Staniford-Chen, and B. Tung. "A Common Intrusion Specification Language", CIDF working group document, http://www.gidos.org

.

[4]D. Schnackenberg, K. Djahandari, and D. Sterne. "Infrastructure for Intrusion Detection and Response," In *Proceedings of the DARPA Information SurvivabilityConference and Exposition*, Hilton Head, SC, January 2000.

[5] Joseph Barrus,Neil C. Rowe, "distributed autonomous-agent network-intrusion detection and response system", Procedings of the 1998 Command and Control Research and Technology Symposium, Monterey CA, June-July 1998.

[6] Xinyuan Wang, Douglas S. Reeves, S. Felix Wu, "Tracing Based Active Intrusion Response", Journal of Warfare, 1997

[7] K.L.Calvert, S. hattacharjee and E. Zegura, "Directions in Active Networks", IEEE Communication Magazine, 1998 .

[8] John D. Strunk, Garth R. Goodson, Adam G. Pennington, Craig A.N. Soules, Gregory R. Ganger ,"Intrusion Detection, Diagnosis, and Recovery with Self-Securing Storage" May 2002

[9] A. Hess, M. Schoeller, G. Schaefer, M. Zitterbart, and A.Wolisz. A dynamic and flexible Access Control and Resource Monitoring Mechanism for Active Nodes. In *Short Paper Proc. of OpenArch 2002*, pages 11–16, New York, USA, June 2002.

[10] Calvin Ko, Deborah A. Frincke, Terrence Goan Jr, L. Todd Heberlein, Karl Levitt, Biswanath Mukherjee and Christopher Wee. Analysis of An Algorithm for Distributed Recognition and Accountability. 1st ACM Conference on Computer and Communications Security, Dept. of Computer Science, University of California, Davis, November 1993.

[11] Javed Aslam, Sergey Bratus, David Kotz, Ron Peterson, Brett Tofel, Daniela Rus, "The Kerf Toolkit for Intrusion Analysis"IEEE Security & Privacy, pp-42-52, 2004.

Acknowledgements

The author would like to thank Mr. D P Sinha, GM(GP), Head-SPIC, ONGC. My sincere thanks to Mr. MHS Sastry DGM(GP), Mr. N N Jha CG(GP), Mr. NNB Naidu CP(GP), Mr. CPS Rana CG(GP) Mr. K Subhramanyam Manager(Prog.) to inspire me to do this. Thanks also go to my friends and colleagues Mr. D C Rabha, Mr. SSP Singh, Mr. S Rana and last but not the least the wide variety of system equipped in our SPIC centre that helps me to test my work.