ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

BGIDS-Behavioral Graph based Intrusion Detection System

Ajay Poonia[1], J.A. Laxminarayana
Dept. of Computer Enigneering
Goa College of Engineering, Farmagudi, Goa, India

Abstract: Security is an important concern in every field of computing. Specifically, security is a process of creating the system that is secure from all forms of attacks and intrusions. For detecting the intrusion, we have various types of Intrusion Detection System (IDS). The commonly used types of intrusion detection system are the network based intrusion detection system and host based intrusion detection system. But host based IDS solely monitors the host whereas network based IDS solely monitors the network. In detecting the intrusion, both the host activity and network activity must be monitored simultaneously. This paper presents a technique of monitoring both the host and the network at the same time. The BGIDS is the synthesis of both the behavior based IDS for monitoring the host and graph based IDS for monitoring the network.

Keywords: Intrusion Detection, Anomaly, Network, Graph, Signature.

I. INTRODUCTION

Intrusion detection system monitors the targeted system and network resources for any malicious activity. It checks and monitors computers and/or networks to identify suspicious activity. When the IDS detects any suspicious activity with a computer and/or a network, it raises an alert.

IDSs have been classified into two types signature-based and anomaly-based. A signature-based (or misuse-based) IDS maintain a database of attack signatures. It works similarly to anti-virus software, by raising an alert when it matches one of the signatures. These signatures typically address applications or systems for which security vulnerabilities are already known. Similarly like antivirus software which fails to detect viruses when there is no signature available in the database or the virus database is out of date, a signature-based IDS also fails to detect unknown attacks.

To overcome the limitation of signature-based IDSs, researchers have developed other ways to detect intrusions. An anomaly-based IDS works by first building a statistical model of usage patterns describing the normal behavior of phase is completed, the system then uses a similarity metric to compare new input requests with the model stored in the database, and generates alerts for those requests that are deviating significantly, considering them as a malicious activity. An attack is detected because the request produces a malicious behavior than what was observed when creating the model. The main advantage of an anomaly-based system is its ability to detect previously unknown (or variants of known) attacks when they appear. The drawback of these systems is that it produces high rates of false positives and can be evaded using mimicry attacks, i.e., attempts to pass as normal behavior.

These types of IDS are further divided into two types of IDS, based on the resources it monitors. They are Host based IDS and Network based IDS.

Host based intrusion detection (HIDS) refers to intrusion detection that takes place on an individual host system or application. Currently, HIDS involves installing a sensor on the local host that monitors and reports on the system configuration and application activity. Some common activities of HIDS systems include event correlation, log analysis, policy enforcement, integrity checking, root-kit detection, and alerting. They often also have the ability to baseline a host system to detect variations in system configuration.

A network intrusion detection system (NIDS) is a system, which detects intrusions on network. The word network is used for this system, because it monitors every packet on a network wire and its main objective is to find out whether an attacker is breaking into your system. A network intrusion detection system is mostly place at strategic points in a network. It continuously monitors the traffic on the network to detect any signs of different malicious activity. NIDS involves installing a sensor on the network that monitors and reports on the network configuration and activity.

Though they both have the same objective, but they approach this goal in a very different ways. Also, these types of systems are designed to look for separate classifications of things. Therefore, holding the two side by side, evaluating them in hopes of determining a winner is inappropriate. The host-based systems do offer an approach that scales better, but implementing this type of intrusion detection system requires a high degree of expertise about the operating system that the sensors will run on .Also, the lack of cross-platform support is a considerable problem. On the other hand, network-based solutions are easier to implement and are more portable, but have the growing problem that they cannot keep up with heavy traffic or with high network speeds. From an attack perspective, the situation is similar. Network-based intrusion detection systems are appealing because of the way they inspect traffic, “network monitors can see evidence of certain classes of traffic that are not visible to host-based systems”,[1]. Attacks from malformed or “formulated” packets, packet storms, and many denials of service attacks can only be discovered with the help of sensors which are placed on the network. Host-based systems, however, offer the counter argument. An attacker attempting to infiltrate a host system may do so through a dial-up connection, which cannot be seen by network monitors, only by a sensor on the target host. Further, only host-based sensors can analyze the results of commands that are executed on an individual host system, which could possibly be a malicious activity or simply against a security

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

policy. In many ways, neither method offers a complete intrusion detection solution.

The best solution is one that will incorporate advantages of both methods. A system that integrates both host and network based characteristics seems intuitively the most logical approach. This paper present a method of monitoring both the host and network simultaneously. The host is monitored locally with help of anomaly/behavioral based IDS and the network is monitored with help of Graph based IDS. So, the BGIDS is the synthesis of both the behavior based IDS for monitoring the host and Graph based IDS for monitoring the network.

II. RELATED WORK

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station

Intruders can broadly divided into three different types:

a. Masquerader
b. Misfeasor
c. Clandestine user

Masquerader are typically outsiders from the trusted users and not authorized to use the computer systems. These penetrate the system protection by way of legitimate user accounts.

Misfeasor is typically insiders and legitimate users who accesses resources that they are not authorized to use. Or, they may be authorized but misuses her privileges.

Clandestine user can be both outsider and insider. This type of intruder gains the supervisory access to the system.

A. Current techniques in IDS:

a. Behavior-based IDS:

Behavior-based intrusion detection techniques assume that an intrusion can be detected by observing an aberration from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means, [3]. The intrusion detection system later compares this model with the current activity. When a aberration in the behavior is observed, an alarm is generated. Anything that does not correspond to a previously learned behavior is considered intrusive.

b. Nides:

The Next -Generation Intrusion Detection Expert System (NIDES) is the comprehensive enhancement to IDES. NIDES is a real-time intrusion detection application which integrates a statistical analysis based anomaly detector and a rule-based misuse detection system. This combination gives NIDES the ability to detect penetrations from internal and external attacks. SRI incorporated a number of significant improvements into NIDES. In addition to modularizing the application, NIDES includes an enhanced statistical analysis component and additional support for a strict client-server model. NIDES also include a comprehensive user interface that permits access to all of the applications capabilities, as well as a context -sensitive help system. [2]

c. Dids:

The Distributed Intrusion Detection System (DIDS) combines attributes of a network monitoring system with the system-level capabilities of an audit record-based combined anomaly/misuse detector. DIDS incorporates a monitor on each host, a monitor on the local area network (LAN), and a DIDS director. Each host monitor consists of a host event generator and a host agent. The host event generator reviews the audit data from the host for indications of events which may be part of an attack. The DIDS host event generators also utilize user and group profiles to identify anomalous behaviors in the audit record. The information identified by the host event generator is reported to the DIDS director by the host agent.

The LAN monitor is the network equivalent of the host monitor. It includes the LAN event generator and the LAN agent. However, unlike the host event generator, the LAN event generator does not review audit data. The LAN event generator utilizes the network monitoring approach to review all network traffic, including host-to-host connections and resources used. The information obtained by the LAN event generator is reported to the DIDS director by the LAN agent.

The DIDS director forms the heart of the intrusion detection mechanism. It is composed of three components, the communications manager, an expert system and a user interface. The communications manager is receives input from each of the host monitors and from the LAN monitor and forwards the information to the expert system for analysis. The communications manager is also capable of forwarding requests for additional information from the expert system to the host monitors and the LAN monitor. The DIDS expert system is a rule-based system which is responsible to analyzing the information received from the monitors and reporting it to the security official. The final component of the DIDS system, the user interface, allows a security official to interactively review the status of the system, receive reports from the expert system, and request additional security-related information from the system. [2]

d. Stat/Ustat:

The State Transition Analysis Tool (STAT) and USTAT, the variation of STAT which was designed specifically for the UNIX operating system environment, are rule-based penetration detection approaches which characterize the process of an attack on a computer system as a series of transitions from an initial state to a compromised state. The technique defines specific events, called signature actions, which occur between each of the intermediate transitions. The omission of any of the signature actions results in a failed attack on the system. [2]

e. Tripwire:

Tripwire is an integrity checking program which permits a system administrator to monitor system files for addition, deletion, or modification. The program is estimated to have been installed on several thousand systems worldwide. While it is not an intrusion detection mechanism, Tripwire does provide valuable information for the process of detecting attacks on a system. Tripwire utilizes input from a configuration file and a database to identify areas of interest. The configuration file consists of a description of the file systems which are to be monitored. The database contains the signatures of files which match the configuration. The

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

signatures of the files are calculated based on the contents of the system files. The signature computation is easy to derive but impossible to reverse.

Tripwire operates in one of four modes. In the database initialization mode, the program generates a database which contains all of the relevant information on the system files, including signatures. Because the baseline database is being generated based on the files which currently exist in the system, it is critical that the existing database is free of logic bombs, viruses, Trojan horses, or other attack programs.

The integrity checking mode results in the creation of a new database from information contained in the configuration. The information in the new database is compared with the results contained in the original database. Any discrepancies are processed through a filter which determines which file attributes can be changed without adversely affecting the system. The remaining identified changes are then reported to the system administrator. [5]

The final two operating modes are used to ensure that the information in the database is consistent. The database update mode calculates new signatures for those files which have been legitimately changed. In the interactive database update mode the program generates a list of those files which have been modified and updates those which are identified by the system administrator as legitimate.

Tripwire is a good tool for monitoring the status of system files. However, it is limited in its capabilities. Tripwire makes no pretense of insuring the complete security of the computer system. It functions to notify system administrators of a very important indication of an intrusion. This information, combined with other security-related tools, should provide a more secure operating environment.

f. GrIDS:

The Graph-Based Intrusion Detection System (GrIDS) is designed to analyze network activity in large networks for the presence of attacks. GrIDS aggregate the actions of networks users into the activity graphs. Based on a review of the structure of these graphs the system can identify patterns which indicate intrusive behavior. In addition to diagramming the basic network activity, GrIDS incorporates supplementary information in the form of attributes to the tree-like structure of the diagram. Information received from other intrusion detection devices and network monitors can be included in the attributes of the activity graphs.

Individual types of graphs will be maintained in graph spaces with the GrIDS system. Because there are a number of possible attacks on the network, multiple graph spaces must be maintained. Each graph space is dependent on a specific rule set which modifies the graphs within its graph space based on inputs to the system.

GrIDS is able to analyze activity on large networks because of its ability to model networks as a series of hierarchies. Each area within the hierarchy has a GrIDS module which is responsible for that area. Any activity which crosses area boundaries will be passed up to the GrIDS in the next higher level for resolution.

The GrIDS in that level builds reduced graphs which model the underlying structure on a smaller scale. This ability to model sub hierarchies allows GrIDS to monitor networks of increasing complexity. The true promise in the GrIDS system is in its ability to assist users in creating rule sets for the system. [4]

GrIDS include a policy language which enables administrators to translate organizational policies and guidelines into rule sets which are used to analyze the network activity. This technique allows the GrIDS to expand from merely identifying indications of external attacks to detecting any activity which violates established network usage policies. The designers of GrIDS have not attempted to develop a complete intrusion detection device. Instead, they have proposed an innovative technique which addresses elements of intrusion detection which have been largely ignored in the past.

g. Thumb Printing:

Thumb printing is a method of tracking intruders through a sequence of logins, referred to by the authors as a connection chain. While it is not intended to be an independent intrusion detection system, it could prove to be a valuable addition to other technologies. Thumb printing was developed by researchers at the University of California at Davis in response to a weakness in DIDS. Because DIDS is unable to correlate to parts of a connection chain when a user has exited and then reentered outside of the DIDS domain, thumb printing was devised to compare the content of the connections in the chain. Since commands issued by a user should remain the same as they pass through the various hosts in the connection chain, summaries of the content of connection at two points could be compared to determine if they were links in the same chain. The summaries would be generated by passively monitoring the network traffic at each host.

A current weakness in this approach is that it assumes that the content of the connections along the chain are the same. As a result, the use of different encryption techniques by two points would render the method useless. [2]

h. Cooperating Security Manger:

While DIDS takes a centralized security approach to network intrusion detection, Cooperating Security Managers (CSM) decentralizes the process. A separate CSM is run on each computer which is connected to the network.

Each CSM consists of six elements. The heart of the CSM is the Security Manager (SECMGR). The SECMGR receives input from the various CSM components and coordinates with CSM's on other hosts as users pass through the network. The command monitor (CMNDMON) intercepts the commands from the user and forwards them to the host intrusion detection system (IDS). While CSM requires the presence of an intrusion detection system on each host, the actual mechanism is separate from the CSM and can therefore be any intrusion detection tool. Any intrusions detected by the IDS are reported to the SECMGR.

The CSM Intrusion Handler (IH) is one of the distinguishing characteristics of CSM. Instead of simply reporting intrusive activity to a security administrator, the IH can also be configured to take more active measures against an intruder. These include terminating the user's current session, disabling the account being utilized by the alleged intruder, or backing up files which may be modified or deleted by an attacker.

The SECMGR uses TCP to communicate with other CSM's through the communication handler (TCPCOM). CSM only communicates with the CSM immediately before it in the connection chain, not all hosts on the network. Each

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

CSM is responsible for relaying the message through the network.

In addition to addressing the need for detecting intrusive activity in a networked environment, CSM is also scalable and portable because it is not specifically designed for any particular network-wide operating system. Each CSM is unaware of the operating environment on the other CSM's hosts. As long as a CSM has been developed for the operating system which is used on a host, it can be attached to a CSM monitored network.

CSM's ability to utilize a variety of intrusion detection systems also prevents the system from being limited by any of the specific approaches to intrusion detection. As new approaches are developed which more efficiently process user information, they can be incorporated into the CSM, effectively upgrading the CSM as a whole. [3]

III. PROPOSED METHODOLOGY

Below is the architecture of the proposed methodology of BGIDS which can be used for monitoring both the host and the network simultaneously.

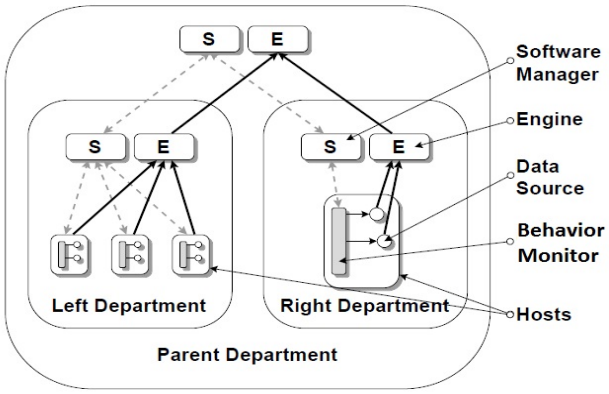

Figure 1 BGIDS architecture

Figure 1 depicts a simple hierarchy with three departments: Left has three hosts, Right has one host and Parent contains Left and Right. There can be any number of hosts in any side of parent department. BGIDS software is in the form of modules with a standardized interface. The modules are started, stopped, and controlled by a Behavior Monitor process located on each host.

Each department has two special modules: the software manager (S) and the graph engine (E). The software manager is responsible for managing the state of the hierarchy and the distributed modules. The hierarchy is re-arranged dynamically by drag-and-drop in a user interface, and starting and stopping particular modules is similarly automated.

BGIDS data sources are modules that monitor activity on networks and send reports of detected activity to the engine. The activity is reported in the form of a node or an edge for possible inclusion in an activity graph. Data sources that are part of BGIDS include network sniffers and point IDSs (intrusion detection systems that work on a single host or LAN). However, BGIDS provides an extensible mechanism such that other security tools can be incorporated as data sources without significant change to them or BGIDS.

The engine builds graphs, and then passes summaries of those graphs up to the engine for its parent department. The parent engine, in turn, builds graphs which have a coarser resolution. In addition to the components shown, there are user interface modules for allowing human interaction with the system, management functions, and display of alerts. There is also a central organizational hierarchy server which has a global view of the topology of the hierarchy, and is responsible for ensuring that changes to the hierarchy happen in a consistent manner.

Hidden Markov Model (HMM) is useful for analyzing the behavior of persons. HMM is also used in making predictions about a person's behavior out of the learned dataset or model. Prediction of behavior means the calculation of the probability of possible actions. The calculation of these predictions of person behavior is based on common algorithms.[6]

The various parameters that are required for analyzing the user behavior are as follows

a) IP of user system.
b) MAC address of user system.
c) Browser used by client.
d) Request rate.
e) Request type.
f) User's operating system.
g) Network Traffic into the user's virtual machine.
h) Network traffic coming out from user's virtual machine.
i) Attempts to access unauthorized memory space.
j) Network spoofing using virtual machine.

Using BGIDS the above mentioned drawbacks of both the host and network based IDS are resolved. We can monitor the host and network at the same time. The security is increased by monitoring both the host and the network. Attacks and intrusion is reduced with the help of BGIDS.

IV. IMPLEMENTATION

Initial approach of this paper is giving encouraging results. We are experimenting out approach with different data sets. A dataset KDD99 is used for the user behavior analysis. This database contains a standard set of data which includes a wide variety of intrusions simulated in a military network environment. This dataset is used as a Model which is compared with user behavior to detect any malicious activity. The implementation is in progress.

V. CONCLUSION

This paper presents technique of monitoring both the host and the network at the same time. The BGIDS is the synthesis of both the behavior based IDS for monitoring the host and Graph based IDS for monitoring the network. BGIDS provides an extensible mechanism such that other security tools can be incorporated as data sources without significant change to the tool or BGIDS.

VI. REFERENCES

[1] Host- vs. Network-Based Intrusion Detection Systems SANS Institute 2000 - 2005

[2] A Comparative Analysis of Current Intrusion Detection Technologies James Cannady Jay Harrell Georgia Institute of Technology Atlanta, Georgia 1996 - polinux.upv.es.

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

[3] Behavioral Intrusion Detection Stefano Zanero Dipartimento di Elettronica e Informazione, Politecnico di Milano, Via Ponzio 34/5, December 9–12, 2008 Milano, Italy.

[4] GrIDS-A GRAPH BASED INTRUSION DETECTION SYSTEM FOR LARGE NETWORKS'S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle Department of Computer Science, university of California, Davis, Davis, CA 95616, S Staniford-chen - 1996.

[5] White, G.B.; Huson, M.L: Cooperating Security Managers: A Peer-Based Intrusion Detection System. MILCOM '96, Conference Proceedings, IEEE Volume: 2, 1996, Page(s): 468 -472 vol.2.

[6] An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols Amrita Anand* Brajesh Patel Department of Computer Science, HOD (M.E), S.R.I.T, Jabalpur, R.G.P.V University, India June 2012

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014