Artificial Intelligence Techniques Applied to Intrusion Detection

Norbik Bashah Idris and Bharanidhran Shanmugam

Abstract – **Intrusion Detection Systems are increasingly a key part of systems defense. Various approaches to Intrusion Detection are currently being used, but they are relatively ineffective. Artificial Intelligence plays a driving role in security services. This paper proposes a dynamic model Intelligent Intrusion Detection System, based on specific AI approach for intrusion detection. The techniques that are being investigated includes neural networks and fuzzy logic with network profiling, that uses simple data mining techniques to process the network data. The proposed system is a hybrid system that combines anomaly, misuse and host based detection. Simple Fuzzy rules, allow us to construct if-then rules that reflect common ways of describing security attacks. For host based intrusion detection we use neural-networks along with self organizing maps. Suspicious intrusions can be traced back to their original source path and any traffic from that particular source will be redirected back to them in future. Both network traffic and system audit data are used as inputs for both.**

Keywords – **Intrusion Detection, Network Security, Data Mining, Fuzzy Logic**

I. Introduction

Information has become an organization's most precious asset. Organizations have become increasingly dependent on it since more information is being stored and processed on network-based systems. The wide spread use of e-commerce, has increased the necessity of protecting the system to a very high extend. Confidentiality, Integrity and availability of information are major concerns in the development and exploitation of network based computer systems. Intrusion Detection System, can detect, prevent and react to the attacks. Intrusion Detection has become an integral part of the information security process. But, it is not technically feasible to build a system with no vulnerabilities; intrusion detection continues to be an important area of research.

The remaining part of this paper is organized as follows: Section II gives an overview of current Intrusion Detection Systems and also about the usage of fuzzy and data mining techniques; Section III elucidates the overview of our proposed architecture. Section IV briefs about the usage of SOM in our proposed model and Section V summarizes the work and points out what we will do in future

CASE-UTM City Campus, Jalan Semarak, Kuala Lumpur, Malaysia-54100 E-mail: bharani@case.utm.my

0-7803-9503-4/05/$20.00 ©2005 IEEE

II. Overview Of Current Intrusion Detection Systems

A. An Overview of Current Intrusion Detection Systems

Intrusion Detection is defined [1] as the process of intelligently monitoring the events occurring in a computer system or network and analyzing them for signs of violations of the security policy. The primary aim of Intrusion Detection Systems (IDS) is to protect the availability, confidentiality and integrity of critical networked information systems. Intrusion Detection Systems (IDS) are defined by both the method used to detect attacks and the placement of the IDS on the network. IDS may perform either misuse detection or anomaly detection and may be deployed as either a network-based system or a host-based system. This results in four general groups: misuse-host, misuse-network, anomaly-host and anomaly-network. Misuse detection relies on matching known patterns of hostile activity against databases of past attacks. They are highly effective at identifying known attack and vulnerabilities, but rather poor in identifying new security threats. Anomaly detection will search for something rare or unusual by applying statistical measures or artificial intelligence to compare current activity against historical knowledge. Common problems with anomaly-based systems are that, they often require extensive training data for artificial learning algorithms, and they tend to be more computationally expensive, because several metrics are often maintained, and these need to be updated against every systems activity. Some IDS combine qualities from all these categories (usually implementing both misuse and anomaly detection) and are known as hybrid systems.

Artificial Intelligence techniques have been applied both to misuse detection and also for anomaly detection. SRI's intrusion Detection Expert System (IDES) [2] encodes an expert's knowledge of known patterns of attack and system vulnerabilities as if-then rules. Time-based Inductive machine (TIM) for intrusion detection [3] learns sequential patterns. Recently, techniques from data mining area have been used to mine normal patterns from audit data [4,5,6]. Several approaches applying artificial neural networks in the intrusion detection system have been proposed [7,8,9]. NeGPAIM [10] based on trend analysis, fuzzy logic and neu-

ral networks to minimize and control intrusion. Existing intrusion detection especially commercial intrusion detection systems that must resist intrusion attacks are based on misuse detection approach, which means these systems will only be able to detect known attack types and in most cases they tend to be ineffective due to various reasons like non-availability of attack patterns, time consumption for developing new attack patterns, insufficient attack data, etc.

B. Computer Attack Categories

DARPA [11] categorizes the attacks into five major types based on the goals and actions of the attacker.

DoS attacks try to make services provided by or to computer users be restricted or denied. For example, SYN-Flood attack, where the attacker floods the victim host with more TCP connection requests than it can handle, causing the host to be unable to respond even to valid requests.

Probe attacks attempt to get information about an existing computer or network configuration.

Remote-to-local (R2L) attacks are caused by an attacker who only has remote access rights. These attacks occur when the attacker tries to get local access to a computer or network

User-to-root(U2R) attacks are performed by an attacker who has rights of user level access and tries to obtain super user access

Data attacks are performed to gain access to some information to which the attacker is not permitted access. Any R2L and U2R has a goal of accessing the secret files.

C. Data Capturing using SNORT

Snort is mainly a so called Network Intrusion Detection system (NIDS), it is Open Source and available for a variety of unices. Snort also can be used as a sniffer to troubleshoot network problems. Basically there are three main modes in which Snort can be configured: sniffer, packet logger and network intrusion detection system. Sniffer mode simply reads the packets off the network and displays them for you in a continuous stream on the console. Packet logger mode logs the packets to the disk. Network intrusion detection mode is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user defined rule set and performs several actions based upon what it sees. We configure Snort in Packet logger mode for our experimental needs.

D. Data Mining and Association Rules

Data Mining is the automated extraction of previously unrealized information from large data sources for the purpose of supporting actions. The recent rapid development in data mining has made available a wide variety of algorithms, drawn from the fields of statistics, pattern recognition, machine learning and databases. Specifically, data mining approaches have been proposed [4,12] and used for anomaly detection. Association rule algorithms find correlations between features or attributes used to describe a data set. The most popular algorithm for mining rules based on two-valued attributes is APRIORI. But this algorithm leads to the problem of categorizing numerical attributes. A solution to this problem was given in [13] by transforming quantitative variables into a set of binary variables by partitioning the domain variables into discrete intervals. This approach, however, suffered from "sharp boundary problem". An alternative solution, [14] using fuzzy, offered smooth transitions from one fuzzy set to another.

E. Fuzzy Logic and Intrusion Detection

Applying fuzzy methods for the development of IDS yields some advantages, compared to classical approach. So, Fuzzy logic techniques have been employed in the computer security field since the early part of 90's. The fuzzy logic provides some flexibility to the uncertain problem of intrusion detection and allows much greater complexity for IDS. Most of the fuzzy IDS require human experts to determine the fuzzy sets and set of fuzzy rules. These tasks are time consuming. However, if the fuzzy rules are automatically generated, less time would be consumed for building a good intrusion classifier and shortens the development time of building or updating an intrusion classifier.

In this paper we propose a mechanism for IDS which utilizes Fuzzy logic along with Data mining technique which is the modified version of FIRE [15] system. The FIRE system uses a simple data-mining algorithm to identify the features that will be helpful in detecting attacks. The security administrator uses the fuzzy sets produced by the system to create fuzzy rules. However, here we will propose a mechanism to automate the rules generation process and reduce the human intervention. AI techniques have also been explored to build intrusion detection systems based on knowledge of past behavior and normal use. They have shown potentiality for anomaly detection with limited ability.

III. Goals And Proposed Architecture

Our aim is to design and develop an Intelligent Intrusion Detection System (IIDS) that would be accurate, low in false alarms, not easily cheated by small variations in patterns, adaptive and be of real time.

In our model we use SNORT [16], a leading and famous open source packet sniffer. The data processor and classifier summarizes and tabulates the data into carefully selected categories i.e. the attack types are carefully correlated. This is the stage where a kind of data mining is performed on the collected data. In the next stage, the current data is compared with the historical mined data to create values that reflect how

new data differs from the past observed data. The inference engine is MySQL based and is bi-directional. Its inference speed is faster than any other text-oriented inference. Based on the facts from the analyzer, the decision will be taken whether to activate the detection phase or not. If the detection phase is activated then an alert will be issued and the tracer phase will be initiated. This phase will trace back to the intruders original source address location. Based on the initial research work we propose a framework for tracing the abnormal packets back to its original source. This tends to be the most tedious phase of the project. Once the original path has been identified and verified then all the attacks from that particular host will be redirected to their source in future. SNORT_INLINE [17] has proved to be the best in changing the appropriate packet values.

A. Attributes

Prior to any data analysis, attributes representing relevant features of the input data (packets) must be established. The set of attributes provided to the Data Analyzer is a subset of all possible attributes pertaining to the information contained in packet headers, packet payloads, as well as aggregate information such as statistics on the number and type of packets or established TCP connections. Attributes are represented by names that will be used as linguistic variables [18] by the Data Miner and the Fuzzy Inference Engine.

B. Data analyzer

Once attributes of relevance have been defined and a data source identified, a Data Analyzer is employed to compute configuration parameters that regulate operation of the IDS. This module analyzes packets and computes aggregate information by grouping packets. Packets can be placed in fixed size groups (s-*group*) or in groups of packets captured in a fixed amount of time (*t-group*). Each s-*group* contains the same number of packets covering a variable time range and each *t-group* contains a variable number of packets captured over a fixed period of time.

C. Rules

Rules are expressed as a logic implication $p \_ q$ where p is called the antecedent of the rule and q is called the consequence of the rule.

D. Traceback framework

The need for tracing the source of the packet is needed for getting the exact information about the intruder [19]. The IDS will be providing information that an exceptional event has occurred, the packet and the time of attack. Once trace back is requested, a query message consisting of the packet, egress

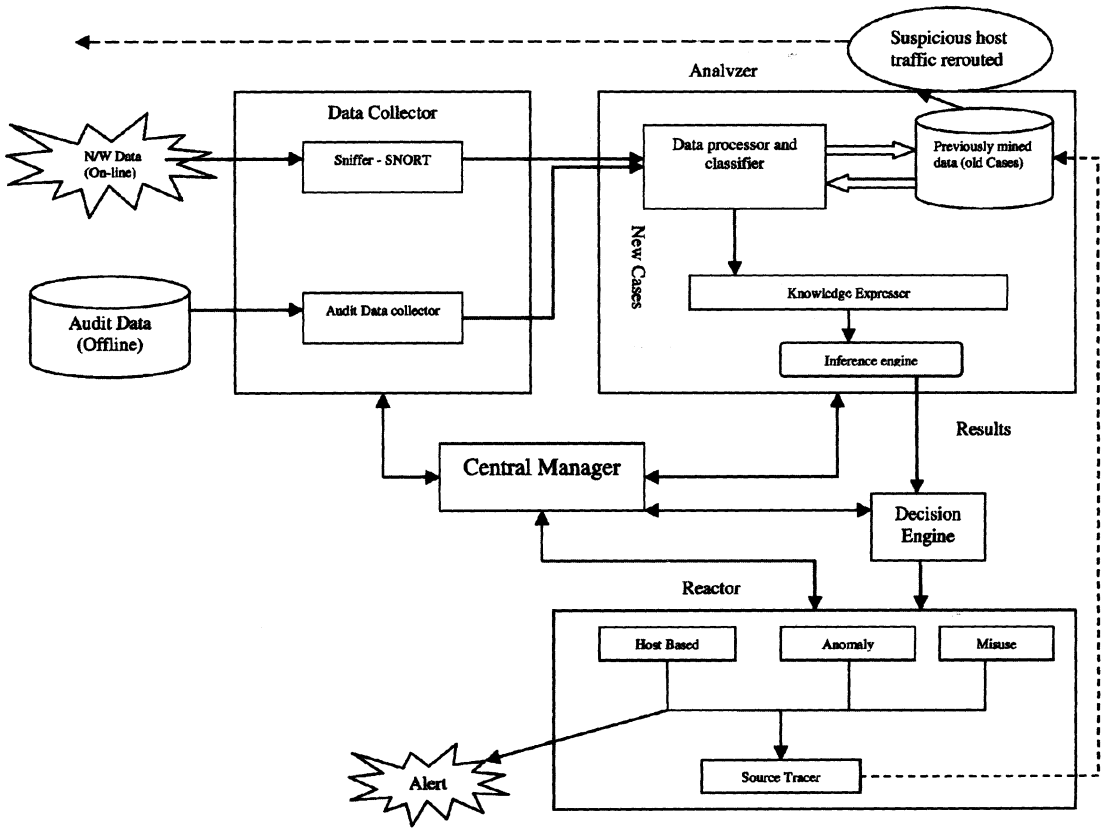

Fig 1. Proposed Architecture

point and the time of receipt is sent to all the Local Data Managers (LDM).Time is critical because this must happen while the appropriate values are still resident at the DC (Data Collector). Once the values are safely transferred to TM, the trace back process will no longer be under real-time constraints. Local Data Manager is responsible for a particular network. Later LDM responds with the partial attack graph and the packet as it entered the region. The attack graph either terminates within the region managed by the LDM, in which a source has been identified, or it contains nodes to the edges of the other LDM network region. Next, TM sends a query to the LDM adjacent of that edge node.

The architecture as shown in Fig.1 is now under construction. Our preliminary research work demonstrates that fuzzy network profiling with data mining can and will provide an efficient solution for Intrusion problems.

IV. Host Based Intrusion Detection

Previous researches have proven that usage of SOM [20] is very efficient in unsupervised learning. In order to fulfill our aim of automating the process of Intrusion detection actions, we first will try to identify the behavior/ characteristic of the common user. The first problem is to establish the nature of initial information on which the rest of the work is based on. Intrusion detection modules may work on a number of different data streams. A lot of systems utilize off-line information (UNIX log-files). In our work, UNIX session information will be used as the features of the system and the characteristics of a common user are defined based on this information. This information is stored for later usage to find out if any user has unusual or different characteristics.

V. Summary And Future Work

A hybrid system has been proposed for aiding network personal in the task of computer intrusion detection. We have combined fuzzy logic with data mining to provide efficient technique for anomaly based intrusion detection and used SOM for host based intrusion detection. This model is now at an infant stage of development. Our long term goal is to make this system implement in a real time environment. More results could be obtained once we finish deploying the system.

Reference

[1] Bace R.G, Intrusion Detection, Technical Publishing (ISBN 1-57870-185-6)

[2] Lunt. T, "Detecting intruders in computer systems", Conference on auditing and computer technology, 1993

[3] Teng H., Chen K., and Lu S., "Adaptive real time anomaly detection using inductively generated sequential patters", IEEE computer society symposium on research in security and privacy, California, IEEE Computer Society 278-84, 1990

[4] Lee, Stolfo S., Mok K., "Mining audit data to build data to build intrusion detection models," Fourth international conference on knowledge discovery and data mining, New York, AAAI Press 66-72, 1998

[5] Mukkamala, R., Gagnon J., Jaiodia S., "Integrating data mining techniques with intrusion detection methods", Research Advances in Database and Information systems security, 33-46, 2000

[6] Stolfo S., Lee, Chanm,"Data mining-based Intrusion detectors : An overview of the Columbia IDS", Project SIGMOD Record, Vol 30, No 4, 2001

[7] Debar, Becker M., Siboni D., "A neural network component for an intrusion detection system," IEEE Computer Society Symposium on Research in Computer Security and Privacy, 240-250, 1992

[8] Tan K., "The Application of Neural Networks to UNIX Computer security", IEEE International conference on Neural Networks Vol 1, 476-481, 1995

[9] Wang J., Wang Z., Dai K., "A Network intrusion detection system based on ANN", InfoSecu04, ACM 2004(ISBN1-58113-955-1)

[10] Botha M., Solms R., Perry K., Loubser E., Yamoyany G., "The utilization of Artificial Intelligence in a Hybrid Intrusion Detection System", SAICSIT, 149-155, 2002

[11] MIT Lincolon Laboratory, 1999 DARPA intrusion detection evaluation design and procedure, DARPA Technical report, Feb 2001

[12] Dokas .P, Ertoz L., Kumar V., Lazarevic A., Srivastava J., Tan P., "Data Mining for Network Intrusion Detection", Proceedings of NSF Workshop on Next Generation Data Mining, 2002

[13] Agrawal R., Srikant R., "Fast algorithms for mining association rules" 20th international conference on very large databases, September 1994

[14] Kuok, C., Fu A., Wong M., "Mining fuzzy association rules in databases", SIGMOD Record 17 (1) 41-46.

[15] Dickerson J E., Dickerson J A., " Fuzzy Network Profiling for Intrusion Detection", Proceedings of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta 2000.

[16] SNORT, www.snort.org

[17] SNORT INLINE, http://snort-inline.sourceforge.net/

[18] Zadeh, L. A., "The concept of a linguistic variable and its application to approximate reasoning, Parts 1, 2, and 3," Information Sciences, 1975, 8:199-249, 8:301-357, 9:43-80.

[19] Yuebin. B, Kobayashi, "Intrusion Detection Systems: Technology and Development," Proceedings of the 17th International Conference on Advanced Information Networking and Applications, Xi'an China, 2003

[20] Hoglund A.J., Hatonen K., Sorvari A.S., " A Computer Host Based User Anomaly Detection System Suing Self Organizing Map", Proceedings of the International Joint Conference on Neural Networks, IEEE IJCNN 2000, Vol 5, pp411-416