Design of a Dynamic Intelligent Intrusion Detection System Model

Vivian Ogochukwu Nwaocha
School of Science and Technology
National Open University of Nigeria, Lagos
webdevee@yahoo.com

Abstract*—Most industries require the internet in order to function effectively. We do our banking online, purchase items online and store a wealth of personal information on the hard drive. Unfortunately, thieves know this, and go to great lengths to get our information. As a growing number of companies are connected over the Internet to branch offices in other parts of the country or world, they expose themselves to potential attacks from other individuals or companies after their trade secrets. This could result in losses in the millions or even billions, if important, confidential information is stolen and ends up in the wrong hands. Thus, several organizations invest a great deal in network security in order to ensure that their systems do not fall prey to attacks. However, the existing intrusion detection systems are restricted in their monitoring functionality and require frequent updates and patches. This study presents a dynamic Intelligent Intrusion Detection System model. The proposed model applies fuzzy logic and data mining techniques and a simultaneous implementation of counter measures as the effective means of dynamic intrusion detection.*

Keywords-arificial intelligence; business, dynamic intelligent intrusion detection system model; information; network; organization; security;

I. INTRODUCTION

The widespread use of information stored and processed on network-based systems in most businesses has increased the necessity of protecting these systems. Most businesses are constantly experiencing new threats and vulnerabilities in their applications. Therefore, trying to keep up with emerging threats, applying patches against known vulnerabilities, updating antivirus software, updating firewall rules and all of the other security measures can have a network or security administrator working 18 hour days, 7 days a week with no vacation (Bradley, 2004). There is a crucial need to address security issues that affect networks. It is equally important to be able to sift through the mountains of potential threats and determine which ones truly affect your network so that your time and resources can be put to the most efficient use.

An Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station (Scarfone et al. 2007). 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. These results in four general groups: misuse-host, misuse-network, anomaly-host and anomaly-network. Typically, Intrusion Detection System, can detect, prevent and react to the attacks. Intrusion Detection has become an integral part of the information security process. However, it is not technically feasible to build a system with no vulnerabilities; as such, intrusion detection continues to be an important area of research. Diverse techniques to Intrusion Detection are currently being used, but they are comparatively unproductive. Artificial Intelligence (AI) plays a driving role in protection services. In this study, a dynamic Intelligent Intrusion Detection System model, based on specific AI approach for intrusion detection is employed. The method that is being explored comprise fuzzy logic with network profiling, which applies simple data mining techniques to process the network data. The proposed hybrid system combines anomaly and misuse detection. By applying this technique, suspicious intrusions can be traced back to its original source and any traffic from that particular source will be redirected back to them in future.

II. OBJECTIVE

This study seeks to design and develop a dynamic intelligent intrusion detection system that would be accurate, low in false alarms, not easily cheated by small variations in patterns, adaptive and respond in real-time.

III. LITERTURE REVIEW

Intrusion Detection Systems have in fact been around for a while and a number of studies have been carried out in this area to enhance its efficacy. Basically, they come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. They are characterized by the method employed to detect attacks and the placement of the Intrusion Detection System (IDS) on the network. Typically, Intrusion Detection Systems (IDSs) may execute either misuse detection or anomaly detection and may be deployed as either a network-based system or a host-based system. Thus, they can be categorized into four major classes: 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 unusual occurrences by applying statistical measures or artificial intelligence methods to compare current activity against historical knowledge. Common problems with anomaly-based systems

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

are that, they often require extensive training data for artificial learning algorithms, and they tend to be computationally expensive, because several metrics are often maintained, and need to be updated against every systems activity. In 1998, Lee, Stolfo S. and Mok K, carried out a research on mining audit data to build intrusion detection models. Mukkamala, Gagnon and Jaiodia explored the integration of data mining techniques with intrusion detection methods (Mukkamala et al. 2000). In 2001, Stolfo S., Lee and Chan studied "Data mining-based Intrusion detectors" in order to produce a summary of the Columbia Intrusion Detection System. Data mining techniques have equally been employed in mining normal patterns for audit data. In his work, Lunt (1993) designed an Intrusion Detection Expert System that encodes an expert's knowledge of known patterns of attack and system vulnerabilities as if-then rules.

Some techniques applying artificial neural networks in the intrusion detection system have been proposed. Debar, Becker and Siboni, designed a neural network component for an intrusion detection system (Debar et al, 1992). Tan carried out a research on the application of neural networks to UNIX Computer security (Tan, 1995). In 2004, Wang J., Wang Z. and Dai, designed a network intrusion detection system based on artificial neural networks. NeGPAIM (Botha et al., 2002) applies trend analysis, fuzzy logic and neural networks to minimize and control intrusions. Intrusion detection systems that are currently available, particularly commercial intrusion detection systems that must resist intrusion attacks are based on misuse detection approach, which implies that these systems will only be able to spot 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.

Compared to the classical approach, several benefits arise from applying fuzzy methods for the development of Intrusion Detection System (IDS). Consequently, Fuzzy logic systems have been employed in the computer security field since the early 90's. This technique provides some flexibility to the uncertain problem of intrusion detection and allows much greater complexity for IDS. Nevertheless, 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 their studies, Dokas, Ertoz, Vipin, Srivatava and Tan (Dokas et al., 2002) suggested a model for building rare class prediction models for identifying known intrusions and their variations and anomaly/outlier detection schemes for detecting novel attacks whose nature is unknown.

The most recent in fuzzy is to use the Markov model. As suggested in Xi et al (2004), a Window Markov model is proposed, the next state in the window equal evaluation to be the next state of time t, so they create Fuzzy window Markov model. As discussed in the work of Gomez and Dasgupta (2002), a technique to generate fuzzy classifiers using genetic algorithms that can detect anomalies and some specific intrusions was proposed. The main idea is to evolve two rules, one for the normal class and other for the abnormal class using a profile data set with information related to the computer network during the normal behavior and during intrusive (abnormal) behavior. Fuzzy preference relation is another method applied to intrusion detection based on fuzzy satisfaction function. This is applied for comparison of attack signatures. Fuzzy signatures (their gamma resolution sets) are combined by fuzzy operators (Manic and Wilamowski, 2001). Yao, Zhao and Saxton in their studies (Yao et al., 2003) proposed a dynamic approach that tries to discover known or unknown intrusion patterns which uses Support Vector Machine (Chen and Wang,2003).A dynamic fuzzy boundary is developed from labeled data for different levels of security needs.

IV. THE PROPOSED FRAMEWORK

This study presents an Intelligent Intrusion Detection System model which utilizes fuzzy logic along with data mining technique. The proposed model is the modified version of FIRE (Dickerson & Dickerson) system. In order to discover the features that would facilitate the detection of attacks the FIRE system employs a simple data-mining algorithm. The security administrator uses the fuzzy sets produced by the system to generate fuzzy rules. Conversely, a mechanism to automate the rule generation process and reduce the human intervention is proposed. Artificial Intelligence 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.

In this model, SNORT (Snort, 2010), an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire is equally employed. It is a 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 works based on Mandami inference mechanism. Based on outcome of previous studies, it can be concluded that this mechanism would suit the research requirements.

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. A framework for tracing the abnormal packets back to its original source based on single packet is proposed. 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 (Snort, 2010) has been proven to be the best in changing the appropriate packet values. Figure 1 below presents the architecture of the proposed model.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

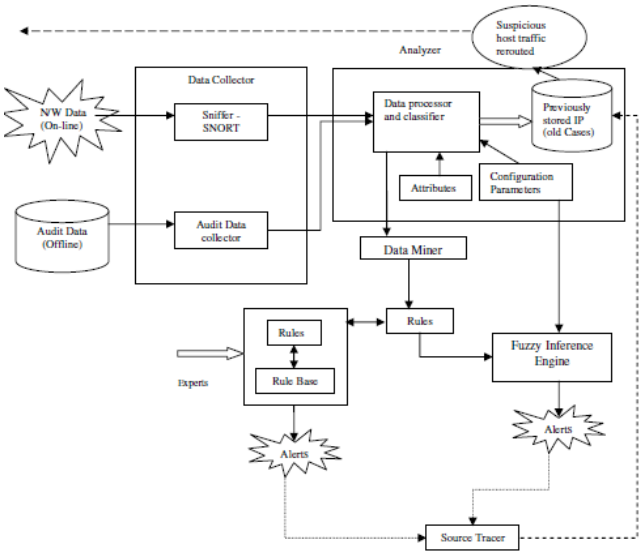

Figure 1: The Framework of a Dynamic Intelligent Detection System Model

The proposed model is a hybrid which comprises fuzzy logic with data mining to provide a more efficient anomaly and misuse intrusion detection in a real-time environment. Attributes representing relevant features of the input data have to be established prior to any data analysis. Once relevant attributes have been defined and data source identified, the Data Analyzer computes configuration parameters that control the operation of the IDS. This module analyzes packets and computes aggregate information by grouping packets. These packets can be placed in permanent 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. 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.

In order to implement the Data Miner a variation of Kuok's algorithm is employed (Kuok et al., 2002). This approach allows for efficient, single–pass, record processing by partitioning data into hierarchical files. To facilitate the discovering of association rules for binary, categorical and numerical attributes, the Apriori is incorporated to Kuok's algorithm. The final output of the algorithm is a set of rules that meet the confidence and support constraints given as input. The tracing of the source of the packet is needed for obtaining the exact information about the intruder. The IDS will be providing information that an exceptional event has occurred, the packet and the time of the attack. Once a trace back is requested, a query message consisting of the packet, egress point and the time of receipt is sent to all the Local Data Managers (LDM).Time is critical as this must take place 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.

V. CONCLUSION AND FUTURE WORK

The goal of this paper is to contribute to the development of network security techniques in general and Network Intrusion Detection System (NIDS) research specifically. The outcome of this study would thus facilitate the task of Network Administrators in particular as well as ensure that businesses and organisations secure their information in order to perform their operations effectively. In this preliminary study a dynamic Intelligent Intrusion Detection System Model has been designed and developed. Nevertheless, the implementation of the overall model has not been done. The future work will thus entail deploying this hybrid system model in a real-time environment as well as applying clustering and classification algorithm in the data mining process to obtain top quality results.

REFERENCES

[1] 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

[2] Bradley T., "Evaluating Threats to your Network". Former Internet/Network Security Guide, 2004

[3] 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

[4] 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.

[5] Dokas P., Ertoz L., Vipin Kumar., Srivastava J., Tan P., "Data Mining for Network Intrusion Detection". National Science Foundation Workshop on Next Generation Data Mining, USA 2002

[6] Gomez J., Dasgupta D., "Evolving Fuzzy classifiers for Intrusion Detection". Proceedings of 2002 IEEE Workshop in Information Assurance, USA NY 2002

[7] Kuok C., Fu A., Wong M., "Mining fuzzy associationrules in databases" SIGMOD Record 17 (1) 41-46, 2002.

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

[9] 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

[10] Manic M., and Wilamowski, "Fuzzy preference approach for Computer Network Attack Detection". IEEE conference on Fuzzy systems 2001

[11] 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

[12] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Center (National Institute of Standards and Technology) (800-94).

[13] SNORT www.snort.org , 2010

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

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

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

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

[17] Xi Z., Sun J., Wenjie L., "Intrusion Detection using Fuzzy Window Markov Model". CCECE Niagra Falls, Canada 2004

[18] Yao TJ, Zhao, Saxton A study on fuzzy intrusion detection, Unpublished work, University of Regina, Canada, 2003

[19] Y. Chen and J.Z. Wang, "Support Vector Learning for Fuzzy Rule-Based Classification Systems", IEEE Transaction on Fuzzy Systems, 2003

AUTHORS PROFILE

Vivian Ogochukwu Nwaocha is currently involved in coordinating Computer Science and Information Technology programs at the National Open University of Nigeria. Her main research interests are network security, artificial intelligence, mobile learning and assistive technologies. A good number of research papers authored by Vivian have been published in various local and international journals. Vivian has equally written a number of books which are accessible online. She has participated in several community and service development projects in Nigeria and beyond. Vivian is a member of Computer Professionals Registration Council of Nigeria, Nigeria Computer Society, Prolearn Academy, elearning Europe, IAENG society of Computer Science, IAENG society of Artificial Intelligence, IAENG society of Bioinformatics and several online social networking communities.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500