International Journal of Scientific and Academic Research (IJSAR) ISSN: 2583-0279
Volume 3, Issue 12, December– 2023
www.ijsar.net
CrossRef DOI: 10.54756/IJSAR.2023.V3.12.1

Robust Design and Implementation of a Network Intrusion Detection System

AYUBA Jumba Gin[1], SANUSI Mohammed[2], JIMOH Abdurrahman Annivbassa[3]

[1,2,3]Electrical /Electronics Engineering, School of Engineering,

Abubakar Tatari Ali Polytechnic Bauchi

Nigeria

ABSTRACT

A Network Intrusion Detection System (NIDS) is an essential component of network security that helps to identify and responds to potential security branches and attacks within a network infrastructure. Computer security has become a challenge and various tools and mechanisms have been developed in order to guarantee a safety level up to the requirements of modern life. Information security is of great concern these days due to the activities of hackers and malicious users on the Internet. Securing information has become a critical issue and is of growing concern as computer systems worldwide become increasingly vulnerable to the rapid increase in the volume of information being transmitted across networks and over the Internet. It describes various approaches of detecting the attacks and preventing the attacks with different techniques such as pattern matching, protocol decoding, defining rules and signatures etc. This research work introduced a technique which provided a robust intrusion detection system against attackers. The framework consists of a Network Intrusion Detection System (NIDS) for detection of traffic to and from a given network, a Host based Intrusion Detection System (HIDS) and a line for possible Intrusion Prevention Systems (IPS). The technique was developed by modeling network using a network simulation software; since a real life implementation is very costly. The result showed that the technique provided an intrusion detection system that can be used to monitor user's activities on the Internet and other networks with relatively minimal error.

Keywords: Cyber security, Hackers, Host Intrusion Detection System, Intrusion Prevention Systems, Network traffic.

1. INTRODUCTION

Security is a major concern in every aspect of our daily life. New methods and equipment are constantly being devised to ensure protection. Computer networks continue to face many threats. Network Intrusion Detection System (NIDS) is a security technology designed to monitor network traffic and detect any unauthorized or malicious activities that may indicate a potential intrusion or attack. It operates by analyzing network pockets and comparing them against known patterns or signatures of known attacks.

Computer systems and networks are protected from abuse by using a defensive measures component known as Intrusion Detection System. Intrusion detection systems (IDSs) analyze information about the activities performed in a computer system or network, looking for evidence of malicious behavior. Attacks against a system manifest themselves in terms of events. These events can be of a different nature and level of granularity. For example, they may be represented by network packets, operating system calls, audit records produced by the operating system auditing facilities, or log messages produced by applications. The goal of intrusion detection systems is to analyze one or more event streams and identify manifestations of attacks.

The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure, one can see that the need for increased network security is vital and important in every organization.

With increasing reliance on computer systems worldwide for data processing and information storage, the need for legitimate security of information and data cannot be overemphasized. Unauthorized access, revelation or destruction of data can violate individual privacy and can even threaten the existence of an organization. Since information is regarded as the live wire of an organization, it is therefore, necessary to secure computer systems and the stored information (Whitman et al, 2012). Information security is a critical need for individuals as well as society and all countries around the world. Network security includes protection methods for all information that is stored and transferred through a system network since the internet era, more and more computers are attacked by viruses, Trojans and also by various kinds of TCP/IP protocol injections. (Henmi et al., 2006).

1.1 STATEMENTS OF THE PROBLEM

Computer networks have brought the world together, by bridging the information gap among people. Network technology has undergone a revolution with better and faster ways of sending information between computers. Unfortunately security systems and policies to govern these networks have not progressed as rapidly. With the birth of the Internet in 1969, computers and computer networks that were isolated from each other were suddenly interconnected. The Internet has grown at an explosive rate with innovations in communication and information technologies. While the Internet has made it easier to reach and communicate with people all over the globe, it has also made it easier to attack computer systems connected to it. With e-commerce and online banking being more and more employed these days, security for systems offering these services has become necessary.

2.0 LITERATURE REVIEW

2.1 Review of the Fundamental Concepts

An intrusion as defined as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource, Balasubramaniyan et al., (2000). Intrusion detection is the technique of determining that an attempt has been made at compromising the resource, or worse the resource has been compromised. One point that needs to be made clear is that, intrusion detection systems (IDSs) do not detect intrusions; they detect evidence or manifestations of intrusions, either while the intrusion is in progress or after an intrusion has occurred.

Intrusion detection started with network-based and host-based systems. Later there were attempts to bring these together into one system. In order to handle large networks, these systems were installed on different parts of the network. But most of these intrusion detection systems (IDSs) have central analysis components. This presents a single point of failure for the whole system. They do not scale well to a distributed network. In addition each intrusion detection system has its own way of reporting, which is usually not compatible with other systems.

2.2 Types of Intrusion Detection System

There are two main types of IDSs: network intrusion detection and host-based intrusion detection.

I. Network Intrusion Detection

Network intrusion detection monitors the packets that are being transmitted through a network. They are also called packet-sniffers. They generally have a signature database against which they compare network packets. These systems have been incapable of operating in switched environments, encrypted networks and high-speed networks.

II. Host-based Intrusion Detection

Host-based intrusion detection systems monitor activity on a host. They are best suited for internal threats because of their ability to monitor and react to specific user actions and file accesses on the host. They offer audit policy management centralization, supply forensics, statistical analysis, and evidentiary support.

III. Hybrid Intrusion Detection

Hybrid intrusion detection systems manage both network-based and host-based systems. They are kind of a central intrusion detection system and add a logical layer to NID and HID.

DOI:10.54756/IJSAR.2023.V3.12.1

2.3 Wireless Sensor Network

A wireless sensor network is an ad-hoc network composed of a large number of small inexpensive devices denoted as nodes (motes). These nodes are battery-operated devices capable of communicating with each other without relying on any fixed infrastructure.

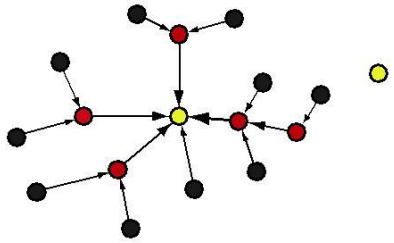

Fig. 1: Wireless sensor

A typical WSN consists of base station and nodes that sense the environment and send data to the base station as shown in figure 1. The base station is more powerful than other nodes and serves as an interface to the outer world. When any node needs to send a message to the base station that is outside of its radio range, it sends it through internal nodes. The internal nodes are the same as others, but besides of local sensing they also provide forwarding service for others.

Nowadays the WSNs are used in many industrial, civilian, environmental and commercial areas. Most of the current WSN applications fall into one of the following classes, (Aravind et al.,2004):

- **Event detection and reporting**

Applications that fall into this class have a common characteristics: the occurrence of the events of interests is not regular. A WSN of such type is expected to be inactive most of the time and activates only when the event occurs.

- **Data gathering and periodic reporting**

These applications are often used to monitor environmental conditions such as temperature, humidity or lighting. These applications usually periodically sense the environment and send measured values to a base stations.

- **Sink initiated querying**

Application of this type, rather than periodically reporting its measurements, waits for a base station (sink) query. That enables the base station (sink) to extract information at a different resolution or granularity, from different regions of space.

- **Tracking-based application**

In many application areas we are interested in tracking the movements of some object. WSNs for this purpose combine some characteristics of the above three classes. For instance, when target is detected, the base station has to be notified promptly (event detection). Then, the base station may initiate queries to receive time-stamped location estimates of target, so it can calculate trajectory (sink-initiated query) and keep querying the appropriate set of sensors.

2.4 Review Of Related Works

There are many of previous studies on the field of network intrusion detection. However, in this study, we focused only on the design of NIDSs and services rather than the detection method used.

Seifedine and Wassim (2008), in their design and implementation of system and network security for an enterprise with world-wide branches, described how the network can be more secured by encrypting the sending data using internet protocol security between user and server. They applied several concepts and showed the actual practices of these concepts through Virtual Private Network (VPN), using a secure tunnel protocol and makes the virtual connection between user and company connected through remote access.

Ibrahim et al., (2012) proposed a technique that uses two different approaches to intrusion detection system, phase and level approaches. The phase approach comprises three phases. Phase 1 accepts the input data and check if it is an attack, phase 2 classifies the attack while phase 3 records the attack into the appropriate classification type. The level approach also has 3 stags. Level 1 detects normal and attack profiles, level 2 records and classifies the attacks into 4 categories; level 3 classifies each attack type and records them. However, the model did not address the problem of countering intrusion attacks. In situations where there

DOI:10.54756/IJSAR.2023.V3.12.1

are intensive attacks, not only will actual alerts be mixed with false alerts, but the amount of alerts will also become unmanageable.

Smiriti and Nishi (2014) defined Firewalls as core elements in network security. A firewall element determines whether to accept or discard a packet that passes through it based on its policy. Firewall allows separation between frontend and backend entity so as to ensure security. A firewall is software or hardware based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. Due to the increasing threat of network attacks, firewall has become reinvestigated, and feature extraction utilities to facilitate the examination of some properties of some selected sets of alerts.

Aakanksha (2016) employed distributed firewall for network security. Distributed Firewall is a host-resident security software application that protects the enterprise network's servers and end-user machines against unwanted intrusion. It is a mechanism to enforce a network domain security policy through the use of a policy Language, policy distribution scheme enabling policy control from a central point and certificates, enabling the identification of any member of the network policy domain. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate. It filters traffic from both the Internet and the internal network. They provide unlimited scalability and also they overcome the single point of failure problem presented by the perimeter firewall.

Ramandeep and Amritpal (2017) examined several Internet-centric firewall designs in an attempt to meet security and performance requirements of multitier applications and by deploying firewalls in series, they were able to significantly increase the difficulty of obtaining unauthorized access to sensitive resources from the network.

3.0 METHODOLOGY

The methodology proposed in this study consisted of collecting and pre-processing network data, designing and building a hardware-based machine learning IDS prototype, and performing the analysis. To collect the data, a small packet sniffer was used. The data was pre-processed and normalized. Finally, using the normalized train and test sets, the IDS prototype was tested and an analysis of the results was performed.

3.1 Intrusion Detection System Architecture

When implementing an Intrusion detection system, it is not possible to completely resort to a common standard due to varying requirements when utilizing the gathering of the data and its analysis. Nevertheless, almost all of them have some basic components/modules that they all share. These components are:

- Data gathering: used for monitoring the source environment. The data gathering is performed using different sensors that observe a specific application or protocol.
- Detection engine: is a module that performs the comparison between the gathered data and the defined rules set and raises alarms in case a deviation is found.
- Database: is a storage module that contains the rule-sets or the IDs which the detector uses when comparing the received data.
- Output: When an alarm is raised, a proper action is taken. This could be an active response where the IDS performs a predefined action such as drop the packet, or an inactive response such as logging for later inspection by a human factor to determine the appropriate response.

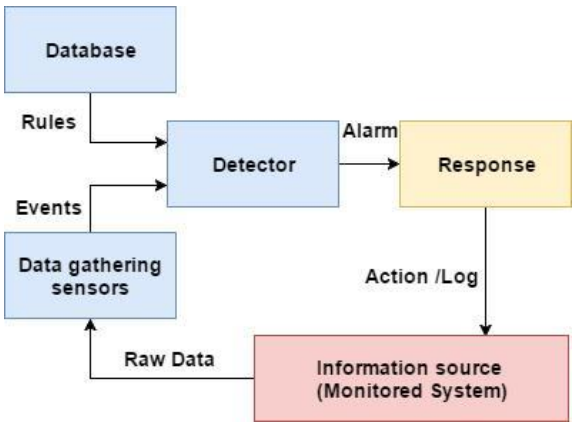

Fig. 2: Intrusion detection system architecture

We use Snort, an IDS/IPS to explain how a generic IDS works. Figure 3 shows the architecture of Snort. It can be seen that; the packet arrives from the network where it is collected by the sniffer module. The packet is then sent to the pre-processor that inspects the type of the packet the detection engine will deal with. This information together with the packet are then forwarded to

DOI:10.54756/IJSAR.2023.V3.12.1

the detection engine that compares the internal component of this packet with the pre-defined rule set stored. Based on the decision of the detection engine an alert is raised and logged in the log database.

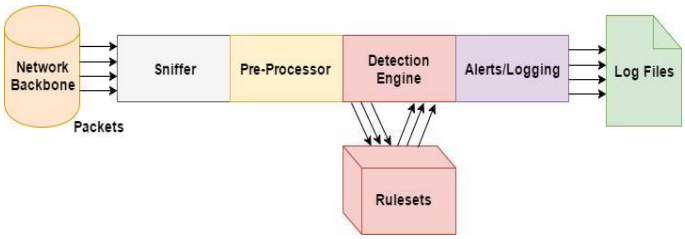

Fig. 3: Snort IDS

3.2 DATA ANALYSIS TECHNIQUES

There are three main types of intrusion detection approaches: Anomaly-based detection, signature-based detection and specification-based detection. In this section, these diff erent paradigms are explained in greater detail.

i. Signature-based detection observes the messages and tries to find pre-defined pat-terns or sequences. These patterns are also known as signatures. The Signatures can mainly define two kinds of lists, a white-list or a black list. In the white list, we only define the kind of messages that are allowed in the system and in the blacklist we define the types of patterns and messages that are not allowed to access the system.

ii. Anomaly-based detection: In anomaly detection, it observed the behaviour of the system. For this, it needs to define an abnormal attitude that will be considered as suspicious. This is similar to the blacklisting approach in the signature based, however, in anomaly based we defined a behaviour that can have a much broader scope and result in detecting behaviour that has never been seen before.

3.3 MESSAGE ENCRYPTION AND SIGNING

The lack of confidentiality of transferred messages can be solved by applying "end-to-end" encryption. This solution, however, needs to be carefully designed. The nodes have limited processing power and cryptographic solutions need to be as lightweight as possible in order to prevent an extensive latency, which could impair the communication on the system.

Adding cryptographic signatures to the transferred messages is one solution to ensure integrity while appending a layer of encryption ensures the confidentiality of the messages.

3.4 NODE AUTHENTICATION

Node authentication, encryption and signing is a measure that can lower the risk of a possible attack on the system. Preliminary research has been done and explained in (Cho and Shin, 2016), which states, that if a security measure has been taken and implemented in an ECU and the attacker is capable to compromise that ECU, the attacker then has access to the data stored in the memory, including all the data that is related to these security measures, such as encryption keys. Moreover, the attacker has the ability to disable such measures by flashing the firmware as demonstrated in (Miller and Valasek, 2015).

3.5 SPECIFICATION-BASED DETECTION

In specification based intrusion detection system, a set of properties, that are extracted from the protocol design are defined for the monitoring purpose i.e. we know the correct system behaviour and can specify it in rules. The classification and detection is then performed by observing a deviation of the execution from the defined properties.

3.6 SYSTEM DESIGN AND STRUCTURE

With the resources available, it proposed the use of software-based IDS embedded in a single ECU. An *IDS node* is a dedicated ECU that listens to messages and monitors one domain or more. An IDS node is expected to have a list of generic functionalities regardless of the approach it follows to perform the detection. The generic functionalities for an IDS node are:

1. Sniffing: Receive all the messages that were sent on the bus.
2. Filtering.
3. Decision making: Process each message based on its ID.
4. Logging.

DOI:10.54756/IJSAR.2023.V3.12.1

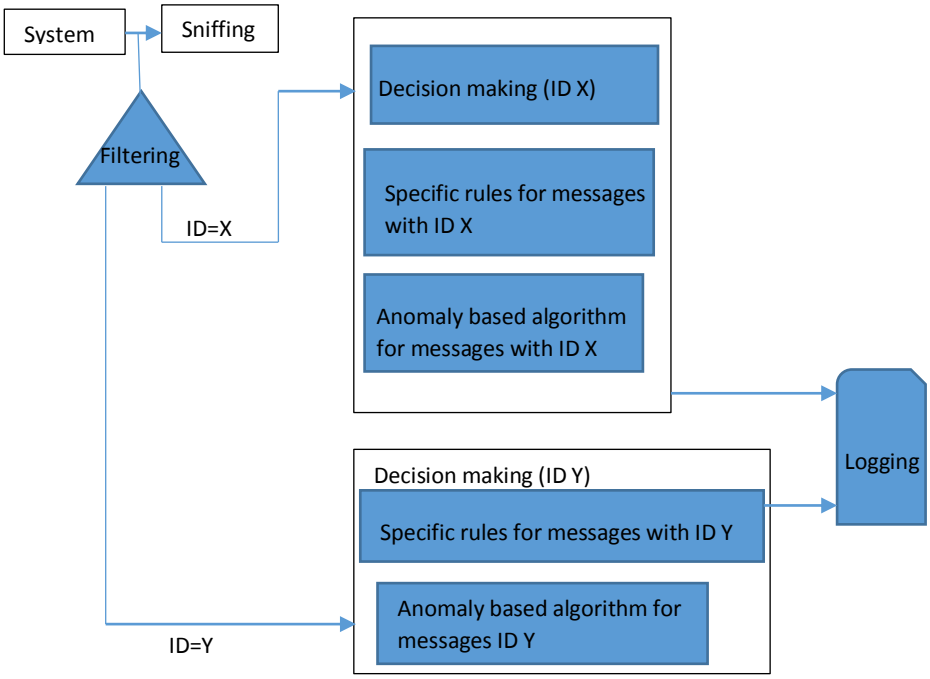

Fig. 4: Architecture of IDS

4.0 RESULTS AND DISCUSSION

We present an overview of the performance of the developed intrusion detection system (IDS). We performed a set of attacks and observed the behavior of the system, while having an active intrusion detection system node.

We performed a test on attack by injecting messages in a specific domain. The injected messages are combination of normal messages that follow the signal database specification and malformed messages that have one or more parameters changed. The type of changed parameters is shown in table 1.

Table 1: Evaluation results for message parameter

Parameter changed	Detection rate (%)
Data length	100
Signal bit length	100
Constant signal byte value	100
Unauthorized messages	100

As presented in table 1, the result of this evaluation show a 100 present detection rate. Such high detection rate is due to the nature of the rules, as they performed a direct comparison between the message properties and the rules extracted from the signal database.

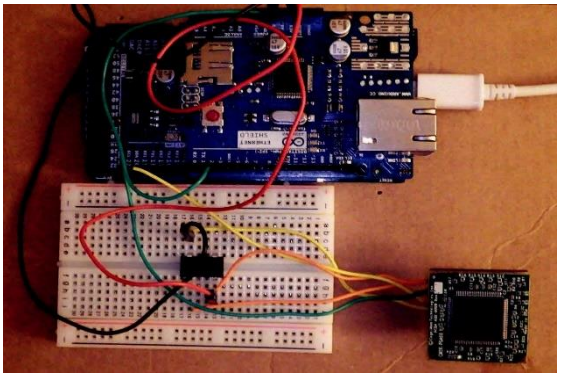

Fig. 5: Hardware Implementation

DOI:10.54756/IJSAR.2023.V3.12.1

The above picture is the prototype embedded system. The Arduino Uno board is connected to the CM 1K via serial I communication protocol.

5.0 SUMMARY

Current IDS testing techniques to data are becoming increasingly complex. There are no testing standards that can quantify the performance of IDS in terms scalability, data handling rate, time to detect an attack, etc. Current IDS heavily rely on unencrypted audit trails and if the data is encrypted this might hinder the performance or even the IDS might become absolute in terms of detecting intrusions.

5.1 CONCLUSION

Using our IDS, different types of attacks can be detected, including message with properties deviating from the signal database and arbitrary message injection. The solution has some limitations, as it is still in the prototype phase. Additionally, for a broader coverage of the network and for a more efficient performance, our work suggests having a dedicated ECU that performs the monitoring in each domain, which on the other hand results in a very high production cost for the manufacturer. Therefore, the cost constrain remains an open issue that needs to be addressed in future works. However, the implementation still has room for the following improvements:

- Security is required for the communication mechanism between hosts.
- There must be a technique for authenticating detectors and system components to each other. This should be practical enough to be applied to a distributed system.
- The latest detectors have to be integrated into the system.

REFERENCES

Alese, Boniface K. &Adu, Michael K. (2014). Curbing Cybercrime by Application of Internet Users' Identification System in Nigeria. World Academy of Science, Engineering and Technology. International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol: 8, No: 9, 2014.

Aakanksha Chopra (2016). Security Issues of Firewall. International Journal of P2P Network Trends and Technology (IJPTT). Vol. 6, Issue 1, January to February, 2016.

H. M. Song, H. R. Kim, and H. K. Kim. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In *2016 International Conference on Information Networking, ICOIN 2016, Kota Kinabalu, Malaysia, January 13-15, 2016*, pages 63–68, 2016.

Rahul Pareek (2011). Network Security: An Approach towards Secure Computing. Journal of Global Research in Computer Science. Vol. 2, No.7, July 2011.

M. S. Hoque, M. A. Mukit, M. A. Bikas, An implementation of intrusion detection system using genetic algorithm, Int. J. of Netw. Security & Its Applications, IV(2012) 111–112.

Ramandeep Kaur & Amritpal Kaur (2017). Safeguard of Security: Firewalls. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 5. Issue 3, March 2017.

Seifedine Kadry &Wassim Hassan (2008). Design and Implementation of System and Network Security for an Enterprise with World Wide Branches. Journal of Theoretical and Applied Information Technology.

Shilpa Pareek, Ashutosh Gautam & Ratul Dey (2017). Different Types Network Security Threats and Solutions; A Review. International Journal of Computer Science, Volume 5, Issue 4, April 2017.

Tung Tran, Ehab Al-Shaer&RaoufBoutaba (2007). PolicyVis: Firewall Security Policy Visualization and Inspection. 21st Large Installation System Administration Conference (LISA). University of Waterloo, Canada.

S. Balasubramanian. An architecture for protection of network hosts from denial of service attacks. Master of Science Thesis. Computer and Information Science and Engineering. University of Florida, Gainesville, FL, 2000.

T. M. Wu, Intrusion Detection Systems, sixth ed., Intrusion Assurance Technology Analysis Center, Herndon, VA, 2009. Accessed September 15, 2013

C. Author: Ayubaj2014@gmail.com

DOI:10.54756/IJSAR.2023.V3.12.1