A Reviewof Effectiveness of Tracing Based Active Intrusion Response Algorithms in Detecting Network Intrusion

[1*]Babalola, M.F., [2*]Omotosho, F.S. & [3*]Agbaje, I.O.
[1]Department of Computer Science, The Polytechnic, Ibadan. Oyo Sate, Nigeria.
[2]Departmentof Computer Science, KwaraState University, Malete, Kwars State, Nigeria.
[3]Department Computer Science, Caleb University, Imota, Lagos State, Nigeria.
E-mails: [1]floxymbabs@gmail; [2]funshosegun@yahoo.com; [3]isaiahagbaje@yahoo.com
Phones: [1]+2348052236814; [2]+2348034016984; [3]+2348061513547

ABSTRACT

The use of computer network technology in all spheres of human endeavors be it in business, social media and academic activities has greatly increased. Due to this excessive use of computer network, series of security treat has been stages to defraud un-suspected users.The integrity of data, unauthorized access and availability of computer network must be protected from intrusion.Network-based intrusion has become a major threat to today's highly networked information systems because effects of intrusions are disastrous to the network users. Security mechanism such as authentication, cryptography, access control and firewall are used as defense but are unable to detect an intrusion internally and counter it. A wide variety of algorithms have been proposed and implemented for intrusion detection some of these algorithms are; intrusion preventions system (IPS), intrusion response system (IRS) and Tracing based active intrusion response (TBAIR) algorithm. In this researchTracing based active intrusion response (TBAIR) algorithm will be applied as countermeasure and tracking of an intruder activities to determine its effectiveness.

Keyword*: -* Network, Intrusion, Authentication, Cryptography, Security, Algorithm

25th iSTEAMS Trans-Atlantic Multidisciplinary Conference Proceedings ReferenceFormat
Babalola, M. F., Omotosho, F. S. & Agbaje, I. O. (2020): A Review of Effectiveness of Tracing Based Active Intrusion Response Algorithms in Detecting Network Intrusion. Proceedings of the 25th iSTEAMS Trans-Atlantic Multidisciplinary Virtual Conference, Laboratoire Jean Kuntzmann, Universite Laboratoire Jean Kuntzmann, Universite Grenoble, Alpes, France June, 2020. Pp 207-220. www.isteams.net/France2020.

1. INTRODUCTION

The use of software systems, information systems and information and communication technology has tremendously grown in size and complexity. Cyber-attacks and malicious activities are common problems associated withcomputer network today, and they are rapidly becoming a major threat to the security of individual internet user, organizations and government.You can implement measures to reduce your network's vulnerability to unauthorized by using credential. A credential is a piece of knowledge that enables individual access to computer based information systems[1]. User names and passwords are commonly used by people during a log in process to prove identity[2]. Passwords remain the most common mechanism for user authentication in computer security systems. This has various drawbacks, such as bad choices by users and vulnerability to capture [3],[5].Network-based intrusion has become a major threat to today's highly networked information systems because effects of intrusions are disastrous to the network users.

It is therefore imperative to have appropriate Intrusion Detection Systems (IDS) in place to monitor, trace, and analyze system execution[8]. Only then can we hope to identify performance bottlenecks, malicious activities, programming functional, and other performance problem.

2. LITERATURE REVIEW

An Intrusion Detection System

This session presents an overview of computer attacks and some of the techniques employed against intrusion. An intrusion Detection System (IDS) is a defense system, which detects hostile activities in a network, the key point is then to detect and possibly prevent activities that may compromise system security or a hacking attempt in progress[14, 13].However, one key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/ or block a suspected connection.According to Amoroso 2011, intrusion detection is “a process of identifying and responding to malicious activity targeted at computing and networking resources”. One of the variables to be detected could be security breaches and therefore detection of intruder activity would explain such activity better and call for methods of response against an intrusion[15].A wide variety of algorithms have been proposed which can detect and combat with these security threats.

Intrusion Detection Systems

Not only will an effective IDS architecture enhance the IDS but it will also maximize on the bandwidth utilization[9]. This is especially important when it comes to deciding which and how many machines are to be protected.

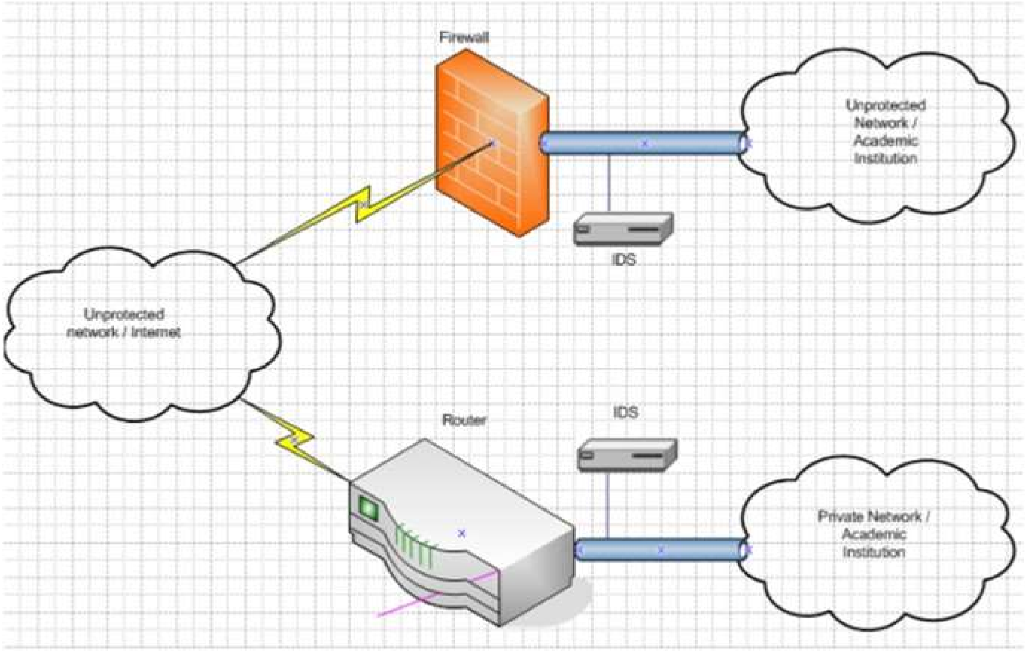
Firewall
Unprotected Network / Academic Institution
IDS
Unprotected network / Internet
Router
IDS
Private Network / Academic Institution

Figure 1: Possible locations of an IDS

There are three basic IDS architectures that have been proposed for intrusion detection systems and they are:
1. Host-based IDS
2. Network-based IDS
3. Distributed IDS

Host-Based Intrusion Detection System (Hids)

A piece of software is loaded onto a system to detect intrusion. The software uses log files or system auditing agents, which look at communication traffic. The software then checks the integrity of system files. Agents are installed on publicly accessible servers such as corporate mail servers or application servers. The agents then report events to a central console that is protected by agent software.

What may be monitored for intrusion detection includes[10, 11]:
1. Log file analyzers - analyzes log files for patterns that indicate intrusion
2. File system monitor - monitors the system to check for integrity of files and directories
3. Connection analyzers - to monitor connection attempts
4. Kernel based analyzer- to detect malicious activity on a kernel

With HIDS the hosts within the private network will have an intrusion detection system that will send alerts to the agent console from where they are analyzed.

Network-Based Intrusion Detection System (NIDS)

Network Intrusion Detection systems (NIDS) monitor the network by capturing network packets. They parse the packets, analyze them and extract useful information from them. The network segment is used as their data sources [14]). All the analysis of the different packets are done without changing or inserting any data on the network. A sensor is used to monitor packets traveling on that particular segment). The IDS determine if the traffic matches any known signatures.

Examples of these known signatures may include:
1. String Signatures— This represents a text string that may indicate a possible network intrusion.
2. Port Signatures— Watches out for connection attempts to well-known ports
3. Header Signatures represent dangerous header combinations that could characterize intrusion.

Distributed Intrusion Detection Systems

Despite their advantages, HIDS and NIDS still have a number of limitations arising from the fact they all have to collect data either from audit trails or by monitoring packets in the network to a centralized location where they are analyzed. And the problems associated with these are [17]:
1. Because of having a centralized analyzer, a single point of failure is introduced. Should the attacker fail the central point, then intrusion detection will be ineffective.
2. There is limited scalability, since after a given limit the central analyzer will not be able to keep up with the flow of traffic.
3. It is difficult to reconfigure or add capabilities to the system since this would require editing a configuration file, adding an entry to a table or installing a new module.
4. The attacker is given the possibility of performing insertion or invasion attacks when analysis of network traffic is done at a single point.

Signature Based NIDS

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious [7] Signatures specify a combination of packet header and packet content inspection rules to identify the anomalous traffic flows. Packet header rule consists of a filter on packets 5-tuple (source and destination IP addresses and ports); content inspection rule consist of a string or regular expressions pattern that has to be matched against the packet payload. While packet header matching requires classification techniques that can be implemented using Ternary Content Addressable Memories (TCAM), pattern matching requires deep packet inspection that involves scanning every byte of the packet payload. Traditionally, patterns have been specified as exact match strings. Naturally, due to their wide adoption and importance, several high speed and efficient string matching algorithms have been proposed recently [12]. These often employ variants of the standard string matching algorithms such as Aho-Corasick, Commentz-Walter and Wu-Manbe and use a preprocessed data-structure to perform high-performance matching. Among these, Aho-Corasick has been adopted most widely.

Regular Expressions Signatures

Regular expressions prove to be fundamentally more efficient and flexible as compared to exact-match strings when specifying signatures for NIDS. The flexibility is due to the high degree of expressiveness achieved by using character classes, union, optional elements, and closures, while the efficiency is due to the effective schemes to perform pattern matching [14]. Open source NIDS systems, such as Snort and Bro, today use regular expressions to specify rules. Regular expressions are also the language of choice in several commercial NIDS products, such as Tipping Point X505 from 3Com and a family of network security appliances from Cisco Systems. Additionally, layer 7 filters based on regular expressions are available for the Linux operating system.

Anomaly Detection Based NIDS

With the description of signature based NIDS, we now focus on anomaly detection for NIDS. Although not yet commercially available, these have been hailed as the future of the NIDS design. The key to the value and effectiveness of anomaly based NIDS is that they can automatically infer attacks which are yet unknown, and therefore undetectable by signature based NIDS. An anomaly detection technique generally consists of two different steps: the first step is called training phase wherein a normal traffic profile is generated; the second phase is called anomaly detection, wherein the learned profile is applied to the current traffic to look for any deviations. A number of anomaly detection mechanisms has been proposed recently to detect such deviations, which can be categorized into statistical methods, data-mining methods and machine learning based methods[8]. We present a brief description of each of them, and introduce some well-known and recent algorithms in each category.

Statistical Anomaly Detection

A large number of statistical schemes assume that an anomaly will result in the deviation of certain traffic characteristics from normal, in terms of the volume (number of bytes, packets, a certain set of IP addresses or ports). Such volume based schemes are successful in identifying large traffic changes such as bandwidth flooding attacks.A number of alternative schemes argue that volume based schemes might not be effective if the attacker is smart enough to keep the disruptions caused by the attacks below certain levels. For example, an attacker can simply reduce the rate at which it is scanning ports, thereby keeping the traffic volume more or less unaffected [6] . Therefore a number of algorithms aim at detecting fine changes in the behavior of traffic and/or the relative distributions of various traffic characteristics. Authors in have proposed to use entropy as a tool to summarize various traffic features.

They show that the analysis of the traffic feature distributions can lead to sophisticated and fairly accurate detection mechanism. It will enable a highly sensitive detection of a wide range of anomalies, which will augment the detections made by the volume-based methods. Authors in propose to use address correlation properties to detect anomalies. Such a scheme examines the packet headers rather than the packet payload, to look for the correlation between various header fields using the wavelet analysis [11, 9].Statistical anomaly detection engines can be added to the signature based systems, in order to automatically detect unknown attacks and possible generate a signature.

Machine Learning to Detect Anomalies

Machine learning is an algorithmic method wherein an application automatically learns from the input and the feedbacks to improve its performance over time[9, 17]. Unlike statistical methods, which aims at determining the deviations in traffic features, machine learning based methods aims at detecting anomalies using some mechanism, and then based upon false positive or not, improving the mechanism.

Data Mining Algorithms to Detect Anomalies

Data mining consists of an advanced set of techniques, that essentially takes a set of data as input and detects the patterns and deviations which is otherwise difficult to detect. Thus, it becomes natural choice to not only detect anomalies, but also to construct the profiles of normal traffic. A number of data mining techniques have been applied.Fuzzy logic algorithms have been employed to use a set of fuzzy sets and rules. In FIRE, the authors propose to use relatively simple data mining techniques to process the network data and generate a set of fuzzy rules for every feature under observation, that will detect individual attacks based on each of the features. FIRE fails to establish any standard model that will represent the current system state; it rather relies on the attack specific rules for the detection. Genetic algorithms, which find approximate solutions to the optimization and search problems, have also been used in anomaly detection [8, 15]. These algorithms are often used to specific features to detect deviations from the normal profile, and based upon the false positive responses, they are also used to fine tune the parameters. Clustering has also been employed to detect anomalies. Clustering is a detection technique to find patterns in data with multiple dimensions. Clustering based system significantly cuts on the amount of training information fed in order to detect anomalies.

Attacks Detected By A Nids

A number of attacks can be detected by current generation of NIDS. Some of these are listed and below.

Scanning Attack

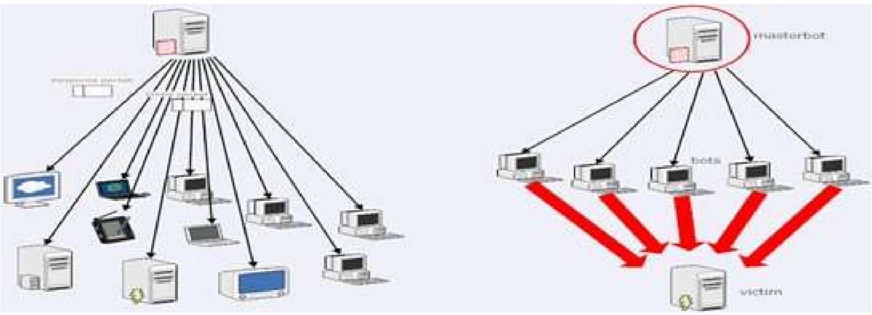

Figure 2: Left diagram shows a scanning attack

Where a single attack host scans a number of victims.Right diagram shows a denial of service attack (DDoS in this case), wherein an attacker uses a number of compromised hosts to attack a given victim.In such attacks, an attacker sends various kinds of packets to probe a system or network for vulnerability that can be exploited [10]. When probe packets are sent the target system responds; the responses are analyzed to determine the characteristics of the target system and if there are vulnerabilities (illustrated in Figure 2). Thus scanning attack essentially identifies a potential victim. Network scanners, port scanners, vulnerability scanners, etc are used to detect and identify the root or the network path of the attack.

The network topology:

- The type of firewall used by the system.
- The identification of hosts that are responding.
- The software, operating systems and server applications that are currently running.
- Vulnerabilities in the system.

Once the victim is identified, the attacker can penetrate them in a specific way. Scanning is typically considered a legal activity and there are a number of examples and applications that employ scanning[15] . The most well-known scanning applications are Web search engines. On the other hand independent individual scan a network or the entire Internet looking for certain information, such as a music or video file. Some well-known malicious scanning include Vertical and Horizontal port scanning, ICMP (ping) scanning, very slow scan, scanning from multiple ports and scanning of multiple IP addresses and ports. NIDS signatures can be devised to identify such malicious scanning activity from a legitimate scanning activity with fairly high degree of accuracy.Denial of Service (DoS) Attacks. A Denial of Service attack attempts to slow down or completely shut down a target so as to disrupt the service and deny the legitimate and authorized users an access. Such attacks are very common in the Internet where a collection of hosts are often used to bombard web servers with dummy requests (illustrated in Figure 3). Such attacks can cause significant economic damage to ecommerce businesses by denying the customers an access to the business. There are a number of different kinds of DoS attacks, some of which are mentioned below.

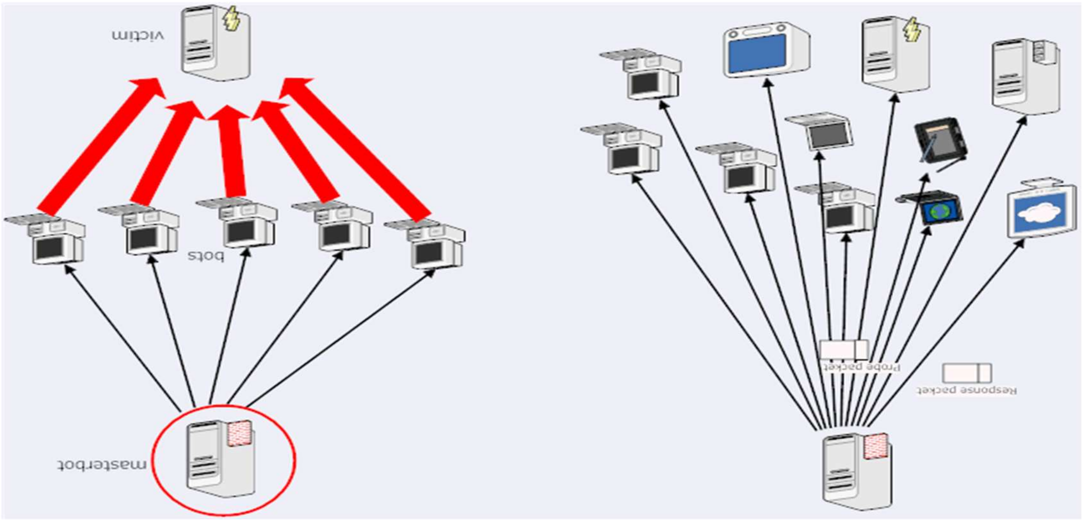

Figure 3: Denial of Service Attack

The IDS could be placed just behind a network firewall or behind perimeter router as shown next on figure 3 to monitor network traffic.

3. ROLE OF TBAIR ON NIDS IN COMBATING ATTACKS

A TBAIR algorithm enables NIDS to detect active, passive attacks, and anomalous conditions, additionally they can also provide a number of key information which can be used to identify the nature of attack, its origin and propagation characteristics [17]. First and foremost, most NIDS often reports the location of the attacker or hacker (from where the attack has been triggered). However, the location is commonly expressed as an IP address, which is not reliable information, as the smart attackers often change the IP address in the attack packets, which is called IP address spoofing.

The key to determine the importance of the source IP address reported by the NIDS is to classify the attack and then determine if the attack requires the reply messages to be seen or not. In attacks where reply packets are required, IP source address spoofing can not be done. In attacks such as a one way DoS flooding attack, the attacker need not examine the reply, and can easily spoof its address. However, Modern NIDS can also report the route that the attack packets have taken. The route information contains key pieces that can be used to trace the hacker in spite of the source address spoofing. A large variety of attacks such as scanning attacks and penetration attacks, etc requires the attacker to examine the reply messages, in which case tracing them becomes much easier[15,17].

Steps By Step Approach (Algorithm) Using Tbair

The main task of TBAIR algorithm as an intrusion detection system is to defend the vulnerability of a system by detecting an attack and possibly repel it. Detecting hostile attacks depends on the number and appropriate action such as;(a) the study of network in question,(b) the type of attack, (c) the root or pathways of the intrusion, hence, Intrusion prevention requires a well-selected combination of “baiting and trapping” aimed at both investigations of threats.

Diverting the intruder’s attention from protected resources is another task. Both the real system and a possible trap system are constantly monitored. Data generated by intrusion detection systems is carefully examined for detection of possible attacks (Intrusions).Once an intrusion has been detected, IDS issues alerts notifying administrators of this fact. The next step is undertaken either by the administrators or the IDS itself, by taking advantage of additional countermeasures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.).

An IDS is an element of the security policy among various IDS tasks, intruder identification is one of the fundamental ones. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources. Intrusion detection may sometimes produce false alarms, for example as a result of malfunctioning network interface or sending attack description or signatures via email[9,14,15,17].

Intrusiondetection System Using TBAIR Model

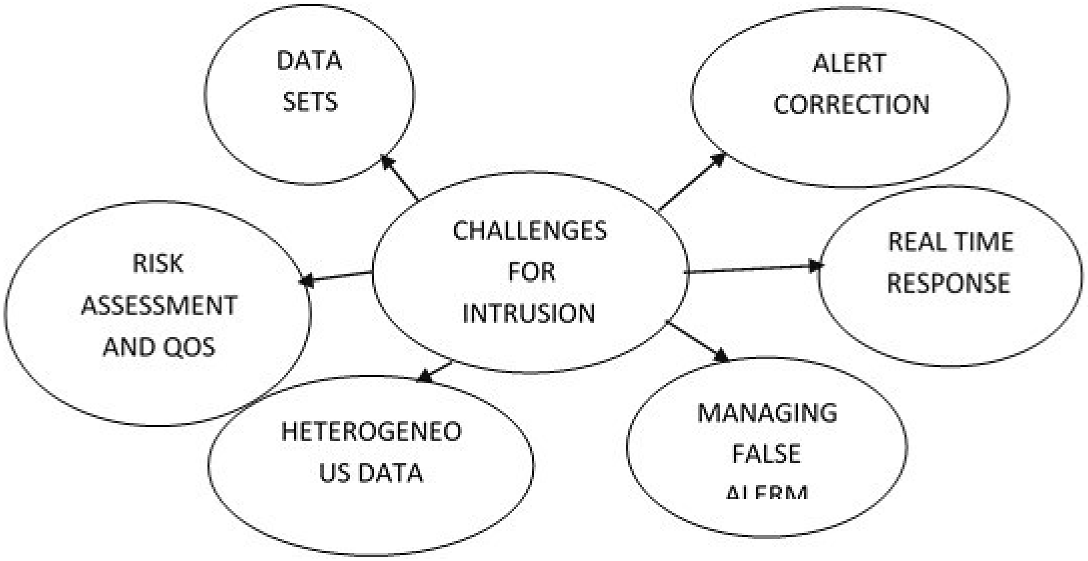

Fig 4: Generic Intrusion Detection System Model

The Data Sets shall be introduce to start the system and TBAIR will consecrate the set and filter it to generate automated response alert/alarm which is been refer to as detection and the message (Real Time Response) will be sent for mitigation through the scene analysis to avoid false alarm and presented such for update and prevention strategies. The Intrusion pattern focused in this case can be categorized in two areas.

1. Passive (aimed at gaining access to penetrate the system without compromising IT resources).
2. Active (results in an unauthorized state change of IT resources).

In most cases, any attempt to take advantage of faults in organization security systems may be considered as an attack and this is the most common symptom of an intrusion.

However, the organization itself may facilitate the task of attackers, using tools which aid in the process of securing its network- so called security and file integrity scanners which can be operated locally(assisting system administrators in vulnerability assessment) or remotely but may also be deliberately used by intruders.

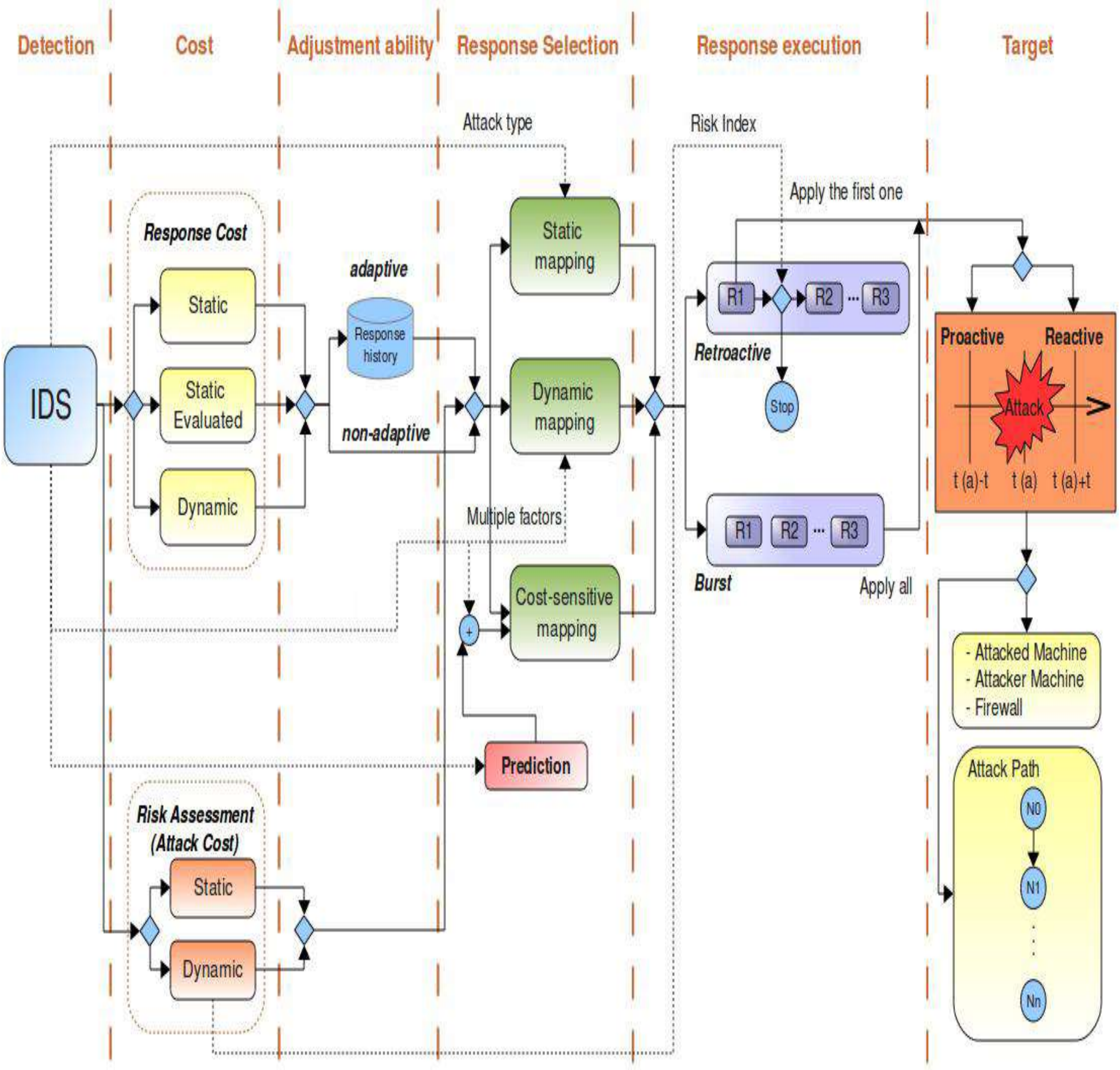

Fig 5: Architecture Design of IDS with the introduction of TBAIR

Architecture Of TBAIR Based

Once a high speed pattern matching architecture has been devised, the other components of NIDS can be built around it. The block schematic diagram of a reference NIDS is shown in Figure 5 above. The protocol analyzer block reassembles a TCP stream, because packets within a TCP streams can arrive out of order, or can be duplicated. Moreover, packets within a TCP flow at a high speed links get multiplexed with packets from other flows, therefore a storage component is required to store the state of a TCP connection upon multiplexing.

In high speed systems, the total number of active TCP connection can reach to a million, therefore the storage component can become a substantial cost driver. Most NIDS are designed only to produce alarms.

Early Warning Mode

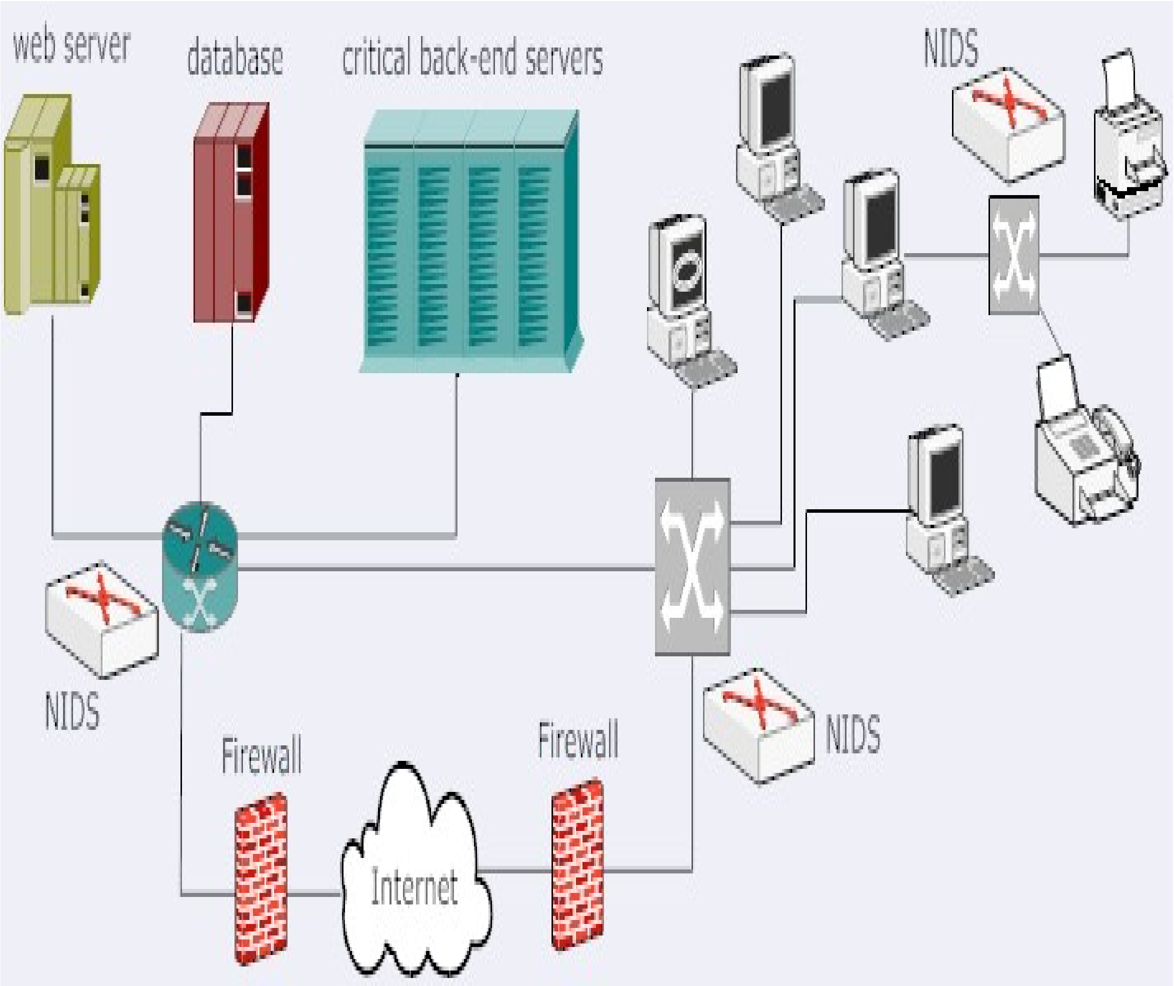

Figure 6: A NIDS as an early detection system.

In such a mode of operation, NIDS are employed outside the perimeter of the firewall (shown in Figure 6 Thus, all traffic entering the host and/or the local/enterprise network is scanned by the NIDS. The key benefit of such configuration is that the NIDS remains at a single locating tapping at a high speed link and can potentially serve a large number of hosts. Thus, the management and update of the signatures and keeping the configurations up-to-date are much easier.

A drawback is that the attacks initiated by the hosts within the firewall perimeter will go undetected. Also, notice that in such architecture, it is possible that the NIDS will raise an alarm while the firewall will block the traffic, thereby effectively rendering the alarm a false one.

Internal Deployments

In such mode of operation, a NIDS is deployed such that it monitors the traffic that traverses any given link within the network, thereby providing an increased security. Thus the NIDS is deployed near the switching nodes within the local network, and near the access routers at the network boundary. In such configurations, the NIDS will no longer monitor the traffic that has been blocked by the firewall, which will lead to a much reduced false alarm rates. A drawback however is that there will be multiple instances of NIDS, and it will become tedious to keep all of them up-to-date in say a large enterprise network. Such configurations are popular in ecommerce back end networks, consisting of web and mail servers and database and storage servers, as an increased security is desirable there. It also aids in keeping an infected server to infect the others within the network.

NIDS Within Every Host

In such configurations, every host has an inbuilt NIDS attached to all of its network interfaces. In a way, such architecture is similar to an anti-virus running on the host; however its key benefit is that the NIDS is decoupled from the host operating system, thus it can be separately managed by the network administrator through a central location. Nevertheless, the management can become complex when the network is large containing several host computers. It has been argued that such structures can lead to difficulty in implementation of the NIDS algorithms as a single instance of NIDS will remain unaware of the traffic traversing through the other links; thus attacks such a Distributed Denial of Service (DDoS) might go undetected.

4. DISCUSSION OF FINDINGS

Basic Sleeping Watermark Tracing Concepts

In order to keep track of network-based intrusions to hosts, it is desirable to monitor hosts through the nearest router or gateways. This is termed a Guardian Gateway.We define the Incoming Guardian Gateway of host H as the nearest router that forwards incoming traffic to H and the Outgoing Guardian Gateway of host H as the nearest router that forwards outgoing traffic from H. It is possible that one host has more than one incoming or outgoing guardian gateway. We define the union of incoming and outgoing guardian gateways of a host as its Guardian Gateway Set (e.g., {GWin1, GWin2, GWout1, GWout2}).

For any guardian gateway set G, we define those hosts as Guarded Host of G whose guardian gateway closure is a subset of G. For a host H, while the traffic between H and its directly connected neighbor hosts does not pass through any gateways, the traffic between H and any non-directly- connected hosts must pass through its guardian gateway closure.We further define a leap as one connection step between hosts within a connection chain (e.g., <Hi , Hi+1>). One leap may consist of multiple hops (or links in the physical network) and the two guardian gateways of the two end hosts. A leap can be specified by a 5-tuple consisting of <protocol number, source ip address, source port number, destination ip address, destination port number>

Now the tracing problem of chained intrusion is defined as discovering and sequencing the guardian gateways of those hosts in the intrusion path, or (equivalently) as finding the leaps along the intrusion path.

The essence of introducing TBAIR technique was to improve the performance of detection rate which can be apply to both static and dynamic of guidance gate way, the host in the intrusion path and the TCP of specific network, thereby reduced the detection response cost, followed by the ability of the adjustment of IDS(Adaptive and Non-Adaptive) which can be reflected in the attack type via the response selection that comprises of static mapping,

Dynamic mapping and cost sensitive mapping that will virtually produce prediction of the attack path.
The prediction of detection can be executed through retroactive and burst in a network with risk index that comprises (R1,R2,R3) and therefore detect the attack path (N0,N1,N2…..Nn).

The specific target network will be reveal from proactive to reactive showing attacked machine, attacker and firewall put in place to curtail the intrusion activities.

Basic Sleeping Watermark Tracing Assumptions
We have identified the following assumptions that motivate and constrain our design:

- Intrusions are interactive and bidirectional,
- Routers are trustworthy and hosts are not trust worthy,
- Each host has a single sleeping watermark tracing (SWT) guardian gateway and
- There is no link-to-link encryption.

The first two assumptions represent our assessments of the nature of the intrusions. Here we refer to intrusions as those attacks aiming to gain unauthorized access, rather than denial of service attacks. A study of CERT security incidents indicates that almost all security incidents, especially unauthorized access incidents, happened at computer hosts rather than routers or gateways. Therefore we believe our assumption to trust routers will cover most intrusion cases. In case there are indeed compromised routers involved in intrusion, the compromised router will be effectively indistinguishable from an attacker. The compromised router needs to be addressed first before the tracing of the intrusion can go any further. In this case SWT can still trace to the farthest trustworthy guardian gateway. s

The assumption of each host having a single SWT guardian gateway is only for simplifying the presentation of the SWT architecture. In case some host has multiple SWT guardian gateways, the guardian gateway set will be used in SWT tracing.

The final assumption represents the inherent limitation of any tracing based on network content. We believe that correlation of encrypted connections in real-time is still an open problem. Without effective intrusion source tracing, intrusion response is limited to the nearby of intrusion target and is passive in front of network-based intrusions. On the other hand, effective intrusion source tracing enables us to build a more active and dynamic intrusion response by pushing the intrusion countermeasures near the source of network-based intrusions. In particular, active network is an emerging framework that seeks to increase the programmability of computer networks and network components. It enables user and application to dynamically control how packets are handled. This customized packet processing opens new ways of network-based intrusion response that were not available in traditional passive networks.

5. CONCLUSION

Tracing Based Active Intrusion Response(TBAIR) technique improved the performance of detection rate which can be apply to both static and dynamic of guidance gate way, the host in the intrusion path and the TCP of specific network, thereby reduced the detection response cost, followed by the ability of the adjustment of IDS(Adaptive and Non-Adaptive) which can be reflected in the attack type via the response selection that comprises of static mapping, Dynamic mapping and cost sensitive mapping that will virtually produce prediction of the attack path.This research study provides a comprehensive explanation of intrusions in terms of their detection and corresponding responses. Emphasis was placed on the development of automatic IRSs to overcome the effects of different intrusions.

REFERENCES

[1] Computer Emergency Response Team (2000), CERT Advisory CA-2000-01 Denial-of Service Development. http://www.cert.org/advisories/CA-2000-01.html.

[2] Jacob, R., (2005) "Intrusion detection systems in wireless ad-hoc networks

[3] Jansen, W., Mell, P.,(2000) detection and intrusion response system. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics at Nashville,Tennessee, pages 2344–2349,.

[4] Lee, W., Fan, W., Miller, M., Stolfo, S., and Zadok, E., (2006) Toward cost-sensitive modeling forwork/olsr/index.phpworm attacks" Master thesis.

[5] Proceedings of the 2003 ACM Workshop on Rapid Malcode, 2003, pp. 11-18.

[6] Ragsdale, D., Carver, C., Humphries, J., and Pooch, U., (2008). Adaptation techniques for intrusion

[7] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., and Zhou, S.,(2007) Specification-response system" Phd thesis, .response using attack graphs in an e-commerce environment. In Proceedings of DSN,

[8] Stakhanova N., (2006) "A framework for adaptive, cost-sensitive intrusion detection

[9] Strasburg, C., (2005) CSI: "A framework for cost-sensitive automated selection of intrusion"

[10] Wang, X.,(3rd edition) (2000) Survivability through Active Intrusion Response. In Proceedings of IEEE Information SurvivabilityWorkshop (ISW-2000).

[11] Wang, Y., Reeves, D., Wu, F., and Yuill, J., (2001) Paris: Sleepy Watermark Tracing: An Active Intrusion Response Framework. In the Proceedings of 16th International Conference of Information Security (IFIP/SEC'01).

[12] Malaysia Computer Emergency Responce Team Incident Statistics. Available online: http://www.mycert.org.my/en/ (accessed on 20 September 2016)

[13] Scarfone, K.; Mell, P.Guide to Intrusion Detection and Prevention Systems (IDPS); Report Number: 800-94; NISTSpecial Publication: Gaithersburg, MD, USA, 2007

[14] Inayat, Z.; Gani, A.; Anuar, N.B.; Khan, M.K.; Anwar, S. Intrusion response systems: Foundations, design, and challenges.J. Netw. Comput.Appl.2016 ,62, 53–74.

[15] Bernaschi, M.; Ferreri, F.; Valcamonici, L. Access points vulnerabilities to DoS attacks in 802.11 networks.Wire. Netw.2008, 14, 159–169.

[16] Hoque, M.S.; Mukit, M.; Bikas, M.; Naser, A. An implementation of intrusion detection system using genetic algorithm.arXiv, 2012; arXiv:1204.1336

[17] Anwar, J.M.Z.S.; Zolkipli, M.F.; Inayat, Z.; Jabir, A.N.; Odili, J.B. Response Option for Attacks Detected by Intrusion Detection System. In Proceedings of the 4th International Conference on Software Engineering and Computer System, Kuantan, Malaysia, 19–21 August 2015; p. 7

A Knowledge Based Document Preparation for Supporting a System Using Artificial Intelligence

Dawodu, A.
Department of Computer Science
D.S. Adegbenro ICT Polytechnic
Itori, Ewekoro, Nigeria
E-mail: babstoncity@gmail.com
Phone: +2348132327110

ABSTRACT

A knowledge based way of preparing documents tools in an organization within an activities such as document preparation that are supported by a knowledge based system. Software called REGENT (Report Generation Tool) works in an environment that generates documents from the reusable document pieces during planning, execution and monitoring the document preparation process in a firm or organizational environment. The documents are built from stored document pieces by using artificial intelligence methods. A system architecture was developed to enable the document generation process to take place within a widen office automation standard. The report preparation process knowledge is captured in form of representing a knowledge based scheme. An artificial intelligence problem solving strategy was developed to take care of reasoning steps when document pieces were being configured. The REGENT environment is normally working when preparing a recurrent report types such as annual reports preparation.

Keywords: knowledge based approach, artificial intelligence, document preparation, office automation, document analysis, document standardization.

25th iSTEAMS Trans-Atlantic Multidisciplinary Conference Proceedings ReferenceFormat
Dawodu, A. (2020): A Knowledge Based Document Preparation for Supporting a System Using Artificial Intelligence. Proceedings of the 25th iSTEAMS Trans-Atlantic Multidisciplinary Virtual Conference, Laboratoire Jean Kuntzmann, Universite Laboratoire Jean Kuntzmann, Universite Grenoble, Alpes, France June, 2020. Pp 195-202. www.isteams.net/France2020.

1. BACKGROUND TO THE STUDY

Artificial Intelligence (AI) is an area of computer science that emphasizes the creation of intelligent machines that works and reacts like humans. Some of the activities with the introduction of artificial intelligence in a computer are speech recognition, planning, learning and problem solving. However, it is evident that there is need to explore the possibilities of incorporating knowledge based advantage in our offices today. The reason is to support the recurring document preparation activities in a cooperative and system settings, such as facilitating the update of yearly reports. The design of such an office automation tool not required to take into account the document processing tools and also how the tool can be integrated with the existing information system software and hardware as well as the existing office procedures that exist in an organization. These include an interface with database systems so as to facilitate the storage and retrieval of data in addition to document pieces.