ANALYSES OF INTRUSION DETECTION AND PREVENTION SYSTEM TOWARD ENHANCING CYBERSPACE SECURITY.

***SHITU ABDULLAHI LAME, *FATIMA ABUBAKAR MAIKUDI, * ALHAJI ADAMU ABDULLAHI AND **YAKUBU MOHAMMED.**
* Department of Computer Science, AD Rufa'I College of Education, Legal & General Studies, Misau. Bauchi State. ** Ministry of Social Welfare and Human Development, Bauchi. Bauchi State.

Abstract
In this study the analyses of intrusion detection and prevention system toward enhancing cyberspace security, public are now capable doing things which were not imaginable few years ago. Information security has become a legitimate concern for both organizations and computer users due to the growing confidence with computers and electronic transactions. The study identify some methodologies thus; Anomaly-based and Stateful Protocol Analysis which will be discussed.

INTRODUCTION
Crime and criminality have been associated with man since his fall. This is why the world of internet today has become a parallel form of life and living. Public are now capable doing things which were not imaginable few years ago. The internet is fast- becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the Mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT is the solutions for the betterment of human kind.
Cybercrime is emerging as a serious threat. Cybercrime a concept which to date has defied a globally accepted definition, appears to be the latest scourge plaguing man and same has occupied the cynosure. The word "Cybercrime is on the lips of almost everyone involved in the use of the computer and internet, be it individual, corporate organization, national, multinational or international." Cybercrimes are relatively a new phenomenon but same has occupied the cynosure of global attention simply because all citizens of the

world, are vulnerable to it, the said vulnerability is almost unavoidable for the fact that the world is in an information age. precisely, cybercrimes emerged with the introduction of the internet, thereby providing a conducive clime for crimes engendered by cybercriminals.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) 1 are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies.

The intrusion prevention is an amalgam of security technologies. Its goal is to anticipate and to stop the attacks [2]. The intrusion prevention is applied by some recent IDS. Instead of analyzing the traffic logs, which lies in discovering the attacks after they took place, the intrusion prevention tries to warn against such attacks. While the systems of intrusion detection try to give the alert, the intrusion prevention systems block the traffic rated dangerous. Over many years, the philosophy of the intrusions detection on the network amounted to detect as many as possible of attacks and possible intrusions and to consign them so that others take the necessary measures. On the contrary, the systems of prevention of the intrusions on the network have been developed in a new philosophy "taking the necessary measures to counter attacks or detectable intrusions with precision" In general terms, the IPS are always online on the network to supervise the traffic and intervene actively by limiting or deleting the traffic judged hostile by interrupting the suspected sessions or by taking other reaction measures to an attack or an intrusion.

CYBER CRIME

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, cybercrime is

committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers. Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

Types of Cybercrime

Most cybercrime falls under two main categories:

- Criminal activity that targets computers
- Criminal activity that uses computers to commit other crimes.

Cybercrime that targets computers often involves viruses and other types of malware.

Cybercriminals may infect computers with viruses and malware to damage devices or stop them working. They may also use malware to delete or steal data.

Cybercrime that stops users using a machine or network, or prevents a business providing a software service to its customers, is called a Denial-of-Service (DoS) attack.

Cybercrime that uses computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images.

Sometimes cybercriminals conduct both categories of cybercrime at once. They may target computers with viruses first. Then, use them to spread malware to other machines or throughout a network.

Cybercriminals may also carry out what is known as a Distributed-Denial-of-Service (DDos) attack. This is similar to a DoS attack but cybercriminals use numerous compromised computers to carry it out.

The US Department of Justice recognizes a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data.

The US has signed the European Convention of Cybercrime. The convention casts a wide net and there are numerous malicious computer-related crimes which it considers cybercrime. For example:

- Illegally intercepting or stealing data.
- Interfering with systems in a way that compromises a network.
- Infringing copyright.
- Illegal gambling.
- Selling illegal items online.
- Soliciting, producing or possessing child pornography.

CHALLENGES IN ESTABLISHING CYBERCRIME

Scams happen in a variety of forms. In cyberspace scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users/to shell out hundreds of money for cyber problems that do not even exist. Any illegal plans to make money falls to scanning. Hacking involve the partial or complete acquisition of certain function with a system, network, or website, it also aims to access to important data and information, breaching privacy. Most hackers attack cooperate and government accounts and there are different time of hacking method and procedures. The following are the reasons of the difficulty of establishing scams and hacking as cybercrimes in the cyberspace:

LACK OF EFFECTIVE REPORTING AND DEARTH OF DATA

As elsewhere pointed out before now that many countries in the world have applicable law and policy against cybercrime but the enforcement of same is a challenge and part of the challenge is not unconnected with lack of effective reporting of incidences of cybercrimes to the appropriate authorities across the globe, in effect, this development has militated against bringing to global attention and appreciation of the extent of the menace of cybercrimes; closely

related to reluctance to disclosure of cybercrimes is the lack of cooperation on the part of the victims, other stake holders and witnesses with police or other agencies saddled with investigation and prosecution of cybercriminals, it is immaterial whether private, corporate or institutional entities are the victims. Several reasons have been advanced for reluctance to report cybercrimes and these includes but not limited to costs arising from follow up of cybercrimes which more often than not far outweigh the benefit derivable thereof, the damage to the reputation and goodwill of Victims especially corporates which are going concerns, of course, the protracted investigation and prosecution which are generally considered as effort and time wasting exercises, more importantly, the difficulty of diligent investigation which is usually scuttled when n a particular cybercrime investigation and prosecution traverses many jurisdictions thereby bringing to the fore issues in approach to cybercrimes.

COST, TIME AND EFFORTS INCURRED IN INVESTIGATION AND PROSECUTION

Given the nature of evidence, that is, forensic, needed in the prosecution of cybercrimes, the cost of same as a scientific crime solving approach as opposed to gathering of evidence in terrestrial crimes is not particularly cheap because of the high-tech equipment, materials and expertise involved to carry out such investigations. With specific reference to business and social interaction, the advent of technology has two pronged outputs, one side represents the numerous advantages which are manifest in the speed and accuracy of information and communications to man wherever he is situate and which development has aptly described the world as one global village, 31 the other dark which has notoriously tagged the dark side, is the unsavoury rise in cybercrimes, when the dark side rears its head, it presents herculean task for investigators and other law enforcement authorities to unravel, given the mass of information that needs scientific examination such as wading through numerous files and breaking encrypted codes, before clues that were intentionally hidden or destroyed, could be sieved out that would possibly lead to arrest and prosecution of cybercriminals at exorbitant costs aside time and efforts of experts which should have been usefully used in other ventures.

LACK OF ADEQUATE LEGISLATION AND INEFFECTIVE ONES WHERE EXTANT

The enforcement of cybercrime laws has largely been hampered due to inadequate legislations and the ineffectiveness of same where there are extant laws in place for cybercrimes. Ajayi 9 According to the United Nations, 32 there are 193 Full UN Members, 2 Observer States and 6 States with partial recognition, making a total of 201 countries in the world. Out of this number, only about 79 countries (Ajayi, 2015), the majority being in Western Europe comprising 47 countries, have laws specifically enacted for cybercrimes; a simple inference that could be drawn from above data is that less than 40% of countries in the world have laws forbidding cybercrime. Given the above scenario of lack of relevant legislations specifically in place for cybercrime, it goes without saying that the development tantamount to giving cybercriminals a license to operate freely without fear but rather with impunity. The absence of requisite laws is even more prevalent in Africa where out of 54 countries 33 constituting the continent, only 4 namely Cameroun, Kenya, South Africa and Zambia (Ajayi, 2015), have laws criminalizing cybercrimes. It is hoped that when the newly enacted African Union Convention on Cyber Security and Personal Data Protection34 comes into force, the lacuna in the law and policy with respect to cybercrimes and other acts incidental thereto, shall be frontally addressed. It is instructive to note that even where there are legislations on cybercrimes, the provisions of the said extant laws are not severe enough to deter cybercriminals from their illegal acts.

INTERNATIONAL LAW WITHOUT ENFORCEMENT MECHANISMS

It is often touted that international law is no law simply because of its lack of enforcement mechanisms; though this assertion is controversial, but the protagonists of this statement insist that, in so far as there, are standing force to implement international laws, they are not persuaded by any argument(s) no matter how convincing, that international law is indeed law in practice.

DOMESTICATION OF INTERNATIONAL LAW AND APPLICABILITY TO SUIT LOCAL CONDITIONS

Generally, it is a legal requirement to the effect that, when presidents or head of states as the case may be, might have signed international treaties, there is need to put in place legislations to make the signed treaties a binding legal instrument at the national level; but very often, the legislature saddled with law making authority neglect this obligation and by so doing, the international treaties or bilateral agreements cannot be enforced by the relevant countries who are parties to treaties.

ILL TRAINED, POORLY PAID AND LACK OF PROTECTION FOR LAW ENFORCEMENT AGENCIES

Cybercriminals are crass opportunists always looking for avenues to make unlawful wealth or in rare cases wreak havoc to computer systems, they have been described as professional thieves and soldiers of fortunes, and above all, cybercriminals are experts in computer and cyberspace issues, thus, the expertise of cybercriminals cannot be juxtaposed with law enforcement agencies who are mere government officials that are ill-trained, poorly remunerated and who offer their services without proper security and protection.

DEARTH OF EXPERTS IN PROSECUTION OF CYBERCRIMES

Related to the above factors of poor training, remuneration and inadequate security and protection on the hazardous job for law enforcement agency officials is the dearth of experts in the prosecution of cybercrimes. It is a well-known fact that, even if the law enforcement agencies had done a good job in the investigation of cybercrime, at the litigation stage, expertise of prosecution attorneys is still very important to secure the conviction of cybercriminal as it is incumbent on prosecution to proof his case beyond doubts; unfortunately, this is not the case as there is dearth of savvy prosecutors in government justice departments.

ABSENCE OF ONE UNIVERSAL LAW GOVERNING CYBERCRIMES

Cybercrimes are borderless, transnational and international crimes and which said cybercrimes are committed in the cyberspace; but the majority of the laws and policies dealing with cybercrimes to date, are either national or regional; the only law specifically dealing with cybercrimes which is international in

character, is the Budapest Convention which for all intents and purposes, is hampered by difficulties associated with international laws.

cybercrimes have only one jurisdiction, that is, the entire world; by so doing, the extant laws and policies which are fragmented, national, regional or quasi-international cannot possibly cope with the problems engendered by cybercrimes; Ipso facto, cybercrime laws shall continue to suffer from enforcement challenges; the only law that can frontally address the menace of cybercrimes, is that law that Would have only one jurisdiction, applicable globally, and not until the political will is mustered to enact that, universal law, mankind shall continue to be plagued by challenges of enforcement posed to cybercrimes laws.

HOW TO PROTECT YOURSELF AGAINST CYBERCRIME

So, now you understand the threat cybercrime represents, what are the best ways to protect your computer and your personal data? Here are our top tips:

I. Keep software and operating system updated

Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.

II. Use anti-virus software and keep it updated

Using anti-virus or a comprehensive internet security solution like Kaspersky Total Security is a smart way to protect your system from attacks.

Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you piece of mind. If you use anti-virus software, make sure you keep it updated to get the best level of protection.

III. Use strong passwords

Be sure to use strong passwords that people cannot guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

IV. Never open attachments in spam emails

A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

V. Do not click on links in spam emails or untrusted websites

Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

VI. Do not give out personal information unless secure

Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.

VII. Contact companies directly about suspicious requests

If you get asked for data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal.

Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialled, they can pretend to be from the bank or other organization that you think you're speaking to.

VIII. Be mindful of which website URLs you visit

Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links with unfamiliar or spammy looking URLs.

If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.

IX. Keep an eye on your bank statements

Our tips should help you avoid falling foul of cybercrime. However, if all else fails, spotting that you have become a victim of cybercrime quickly is important.

Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

Now you understand the threat of cybercrime, protect yourself from it.

IDPS's security capabilities and limitations in

INTRUSION DETECTION AND PROVENTION SYSTEM (IDP) DETECTION METHODOLOGIES

IDPS technologies use many methodologies to detect attacks. The primary methodologies are signature-based, anomaly-based, and stateful protocol analysis. These methodologies are described in detail below.

Signature-Based Detection.

A signature-based IDS (also known as a knowledge-based IDS) examines data traffic in search of patterns that match known signatures—that is, preconfigured, predetermined attack patterns. A signature is a pattern that corresponds to a known attack or type of attack. Signature-based detection is the process of comparing signatures against observed events to identify possible attacks. Examples of signatures are:

- A telnet attempt with a username of "root", which is a violation of an organization's security policy
- An e-mail with a subject of "Free pictures!" and an attachment filename of "freepics.exe", which are characteristics of a known form of malware
- An operating system log entry with a status code value of 645, which indicates that the host's auditing has been disabled Signature-based IDS technology is widely used because many attacks have clear and distinct signatures. The problem with the signature-based approach is that, as new attack strategies are identified, the IDS's database of signatures must be continually updated.

Anomaly-Based Detection

Anomaly-based detection is the process of comparing definitions of normal activity against observed events to identify significant deviations. An IDPS using anomaly based detection has profiles that represent the normal behaviour of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown attacks. For example, suppose that a computer becomes infected with a new type of malware. The malware could consume the computer's processing resources, send many e-mails, initiate large numbers of network connections and perform other behavior that would be significantly different from the established profiles

for the computer. Common problems with anomaly-based detection are inadvertently including malicious activity within a profile, establishing profiles that are not sufficiently complex to reflect real-world computing activity, and generating many false positives.

Stateful Protocol Analysis

Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host- or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used.

The "stateful" in stateful protocol analysis means that the IDPS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state. Stateful protocol analysis can identify unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing another command upon which it is dependent. Another state tracking feature of stateful protocol analysis is that the IDPS can keep track of the authenticator used for each session, and record the authenticator used for suspicious activity. Some IDPSs can also use the authenticator information to define acceptable activity differently for multiple classes of users or specific users.

BENEFITS OF INTRUSION DETECTION SYSTEMS

Intrusion detection systems offer organizations several benefits, starting with the ability to identify security incidents. An IDS can be used to help analyze the quantity and types of attacks. Organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations. These metrics can then be used to assess future risks.

Intrusion detection systems can also help enterprises attain regulatory compliance. An IDS gives companies greater visibility across their networks, making it easier to meet security regulations. Additionally, businesses can use

their IDS logs as part of the documentation to show they are meeting certain compliance requirements.

Intrusion detection systems can also improve security responses. Since IDS sensors can detect network hosts and devices, they can also be used to inspect data within the network packets, as well as identify the OSes of services being used. Using an IDS to collect this information can be much more efficient than manual censuses of connected systems.

CHALLENGES OF INTRUSION DETECTION SYSTEMS

IDSes are prone to false alarms -- or false positives. Consequently, organizations need to fine-tune their IDS products when they first install them. This includes properly configuring their intrusion detection systems to recognize what normal traffic on their network looks like compared to potentially malicious activity.

However, despite the inefficiencies they cause, false positives don't usually cause serious damage to the actual network and simply lead to configuration improvements.

A much more serious IDS mistake is a false negative, which is when the IDS misses a threat and mistakes it for legitimate traffic. In a false negative scenario, IT teams have no indication that an attack is taking place and often don't discover until after the network has been affected in some way. It is better for an IDS to be oversensitive to abnormal behaviors and generate false positives than it is to be under sensitive, generating false negatives.

False negatives are becoming a bigger issue for IDSes -- especially SIDSes -- since malware is evolving and becoming more sophisticated. It's hard to detect a suspected intrusion because new malware may not display the previously detected patterns of suspicious behavior that IDSes are typically designed to detect. As a result, there is an increasing need for IDSes to detect new behavior and proactively identify novel threats and their evasion techniques as soon as possible.

INTRUSION DETECTION (IDS) versus INTRUSION PROTECTION (IPS)

An IPS is similar to an intrusion detection system but differs in that an IPS can be configured to block potential threats. Like intrusion detection systems, IPSes

can be used to monitor, log and report activities, but they can also be configured to stop threats without the involvement of a system administrator. An IDS simply warns of suspicious activity taking place, but it doesn't prevent it.

An IPS is typically located between a company's firewall and the rest of its network and may have the ability to stop any suspected traffic from getting to the rest of the network. Intrusion prevention systems execute responses to active attacks in real time and can actively catch intruders that firewalls or antivirus software may miss.

However, organizations should be careful with IPSes because they can also be prone to false positives. An IPS false positive is likely to be more serious than an IDS false positive because the IPS prevents the legitimate traffic from getting through, whereas the IDS simply flags it as potentially malicious.

It has become a necessity for most organizations to have either an IDS or an IPS -- and usually both -- as part of their security information and event management (SIEM) framework.

Several vendors integrate an IDS and an IPS together in one product -- known as unified threat management (UTM) -- enabling organizations to implement both simultaneously alongside firewalls and systems in their security infrastructure.

CONCLUSION

Information security has become a legitimate concern for both organizations and computer users due to the growing confidence with computers and electronic transactions. Different techniques are used to support the security of an organization against threats or attacks. On the other side, attackers are discovering new techniques and ways to break these security policies. The three detection methodologies discussed so far signature-based, Anomaly-based and Stateful Protocol Analysis, each offer fundamentally different capabilities. Each Methodology offers benefits over the other, such as detecting some attacks that the others cannot, detecting some attacks more accurately, and functioning without significantly impacting the protected hosts' performance.

REFERENCES

Langin, C. L. A SOM+ Diagnostic System for Network Intrusion Detection. Ph.D. Dissertation, Southern Illinois University Carbondale (2011)

Amoroso, E.: Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion.Net Books (1999) [

Abdullah A. Mohamed, "Design Intrusion Detection System Based On Image Block Matching", International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.

K. Scarfone, P. Mell: Special Publication 800-94_ Guide to Intrusion Detection and Prevention Systems (IDPS) (National Institute of Standards and Technology, Gaithersburg 2007)

Ajayi EFG (2016). The Impact of Cybercrimes on Global Trade and Commerce. Available at http://papers.ssrn.comisol3/papers.cfm?abstract_id=2810782 or http://dx.doi.org/10.2139/ssrn.810782

Ajayi EFG (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy. International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://wvvw.ijisc.com/year-2015- issue-2-article-4/

Ben Lutkevich (2021). Intrusion Detection System (IDS). Available at http://techtarget,com/searchsecurity/defination/intrusion-detection-system

I.M. Azhagiri, A. Rajesh and S. Karthik (2015). Intrusion Detection and Prevention System: Technologies and Challenges. International Journal of Applied Engineering Research. ISSN 0973-4562 VOL. 10 NO 87.