THE American Journal of Humanities and Social Sciences Research (THE AJHSSR) 2022

E-ISSN: 2581-8868
Volume-05, Issue-02, pp-01-06
www.theajhssr.com

Research Paper Open Access

THE COMPARATIVE ANALYSIS OF THE INTRUSION DETECTION/INTRUSION PREVENTION SYSTEM

[1]Efiyeseimokumo, [2]Sample Ikeremo
Department of Computer Science, Faculty of Basic and Applied Science, University of Africa, Toru-Orua

ABSTRACT

The speedy improvement of internet usage in this digital economy and globalization which lead to the emerging of e-government, online trade which makes information security become very essential to the safety and economic healthiness to organisation and society that necessitated this comparative analysis of the Intrusion detection/Intrusion prevention system presented in this paper, examined the threat to confidential integrity and availability in information system whereby components of intrusion detection systems / intrusion preventive systems and their functionalities, type of intrusion detection/intrusion preventive systems, types of intrusion detection/intrusion preventive systems techniques, advantages and disadvantages of intrusion detection/intrusion preventive systems techniques and comparatives analysis of intrusion detection/intrusion preventive systems characteristics have been considered. The intrusion detection systems limitation of not be able to preventive occurrence of future attack or preventive measure lead to intrusion preventive systems which have all the capabilities of intrusion detection systems, but because of the advantages and disadvantages that related to the types and techniques used in intrusion detection/intrusion preventive systems, a particular one not can withstand and protect information systems or computer network security from attack. Therefore, combination of four these intrusion detection/ intrusion preventive systems techniques are mostly used in market currently to ensure protection of CIA.

KEYWORDS: Internet, Intrusion detection, Intrusion prevention system, confidential, integrity, availability and information system

1. INTRODUCTION

The rapid growth of internet in this information age and globalization which lead to the emerging of e-government, online trade which include e-Commerce, online banking in the Banking sector, online storage like Cloud computing, crowdsourcing, and e-learning etc that makes society to mostly dependent on information communication Technology (ICT). Organisation or individual dependent on information system to carry out their activities and business like Amazon, ebay, institutions and Banks, which contain vital data, the confidential, integrity and availability of data has to be safe guard from vulnerability and attackers. Hackers, rival competitors, terrorist or international communities may have the intention to carry on attack against these information systems. Hence, information security become very essential to the safety and economic healthiness to organisation and society. Likewise, to uncover privacy gaps, information systems requires all-powerful intrusion detection and prevention systems.

The paper concentrates on the comparative analysis of Intrusion detection / Intrusion prevention system as structured follows 1.Introduction, 2.Literature Review, 3.Type of Intrusion detection/Intrusion prevention systems, 4. Comparative analysis of intrusion detection/ intrusion prevention systems characteristics

1.1 Background

Before figuring out Intrusion detection/ Intrusion prevention systems, one has to comprehend the pattern of action they are try to identify. An Intrusion is the kind of attack on information assets that the attacker try to get access into the system or disorganize usual operation of the system. Patel et al (2010).

Accord to Brown's et al (2002) "*Intrusion are action that attempt to bypass security mechanisms of computer*". These action endanger confidential, integrity and Availability of data and computer networks. Whereas Confidential implies that information not reveal and non-accessible to unauthorized person or organisation,

whereas Integrity implies that data has not change or damage by an unauthorized way and Availability implies that a system containing the requested data can be obtained by real user on request. Sometimes trespass cause by intruder entering the system via internet, computer networks and the affected system operating system, either take advantages of available security weakness of the middleware application which handles the information system. There are two type of attackers, namely insider attacker and the external attacker. The insider attacker are the in-house user that trying to get into unauthorized access and violation of security privileges while external attacker are the ones form outside.

Intrusion detection is the method of checking computer networks for illegal accessing actions either changing of document whereas intrusion prevention is the action of stopping identify system dangers and also stopping them from reaching its target in real time.

2. LITERATURE REVIEW

The literature review will examine scholarly reviews on intrusion detection system and intrusion prevention system,

A lot of scholar has given Intrusion detection/ intrusion prevention system as follows:

i. Intrusion detection systems: is a software or hardware device which automates the trespassing identifying process. Patel (2010). The intrusion detection systems reacts to malicious actions identify in the network or computer system through alert, logging the action or incident either paging the administrator.
ii. Intrusion prevention system: it is a software or hardware device which contains every functions of intrusion detection systems and has the ability to halt future. Patel (2010). The intrusion prevention system has a specific ways of reacting to identify threats and also has the capabilities;

- To reconfigure different security controls in system like firewall either router to stop further attacks.
- To delete suspicious content from attacker and scan away any endangering packet in network traffic.
- To reconfigure different security as well secret management within the browser settings to avoid further attacks.

The Intrusion detection and intrusion prevention system both detect attack or threats in the same way but Nalavade and Meshram (2011) point out that Intrusion prevention technologies are different from intrusion detection system technologies as a result of a particular characteristic its ability to react to detected attack or threat and stopping it from carrying out intended attack also further occurrence, which agreed with the view of Patel (2010) capabilities of intrusion prevention system also in line with the view of Liao et al (2013) that intrusion prevention system is the system that contains every functions of intrusion detection system and ability to halt foresee attacks but Liao et al (2013) described the intrusion detection systems and Intrusion prevention systems as synonyms that the intrusion detection prevention system is hardly been used in the security community. Since Modi et al (2013), Liao et al (2013), Mudzingwa and Agrawal(2012), Faysel and Haque(2010) and Patel, Qassim and wills (2010) agreed on the concept of intrusion detection/ intrusion prevention system that intrusion prevention system have all the capabilities of the intrusion detection systems which Liao et al (2013) described it has synonyms meaning that they are the same but Patel, Qassim and Wills (2010) still insisted that though when the preventive features of intrusion prevention system is disable it become intrusion detection system and that both systems identify malicious and analysing them completely and accurately but difference in the kind of response supplied by any of them.

From the various scholars in the field of intrusion detection/ intrusion prevention system it is obvious that intrusion detection system is limited because it only monitor and detect with response alert, logging and paging administrator whereas intrusion prevention system do all the functions of the intrusion detection system and preventive measurement for stopping further attack. In other word intrusion detection system is passive while intrusion prevention system active or proactive but Faysel and Haqe (2010) Describe intrusion prevention system as premature, meaning research work is still going on, not different in the kind of response supplied by any of them which augured by Patel, Qassim and Wills (2010).

In information security the most important aspect of it is the threat to confidential, integrity and Availability of it source. Hence, in contest of computer network security is to protect CIA from threats or attacks in organisation, government and individual privacy, so efficiency of security measures is the highest priority to any entity, but in the measure of intrusion detection/ intrusion prevention system, the intrusion prevention system is more effective and efficiently because of the preventive measures and performing all the function of the intrusion detection systems. Therefore, intrusion prevention system will be better choice than intrusion detection systems.

2.1. The components of Intrusion detection/Intrusion prevention system

The components of intrusion detection/intrusion prevention system and its functionalities are Mukhopadhyay et al (2011).

- Sensor/Agent: checks and evaluates network events. Sensors is applied for intrusion prevention systems which checks networks, involving network based, wireless and network action evaluating technologies whereas agent is applied for host-based intrusion detection/ intrusion prevention system technologies.
- Database server: it is application of a depository for activities of data storage by the sensors either agents refined by management server.
- Management server: it is a centralized device which accepts evaluates and handles activities information from the sensors/agents it recognizes activities which the sensor/agent cannot.
- Console: it supplies an interface for user and administrators. Console software is normally setup on standard computers which supplies management and checking capabilities.
- The intrusion detection/intrusion prevention systems are been known for various kinds of activities which they are able to identify and the pattern which applied to describe incident are:
- Recording Information: Activity information is normally stored locally, and will transfers to various systems such as centralized logging server, security data, and activity administration solutions, and enterprise management systems.
- Notifying Security Administrators: Alerts or alarms arise if like e-mails, web pages, SNMP traps, syslog messages, and messages on the intrusion detection / intrusion prevention systems user interface, and user-defined programs are identify through the system.
- Producing Report: brief reports of the checked activities and response take through the administrator depended on the feature of specific activities.

3. TYPE OF INTRUSION DETECTION/INTRUSION PREVENTION SYSTEMS

The intrusion detection /intrusion prevention systems carry out extensive logging of information which associated to identifying activities from the network. The logged information are used to affirm the geniuses of alerts examine incidents also compare activities between the intrusion detection/intrusion prevention system and different logging sources. Below are the various types of Intrusion Detection /Intrusion Prevention Systems: -

1. Host-based: checks the features of a particular host and the activities that taking place inside the host or malicious events. Example of such host based intrusion detection/intrusion prevention systems will check including the system logs, network traffic, file access and modification etc. host-based are set up on very demanding hosts like Server that consists of important data and generally accessible server.
2. Network-based: its checks network traffic for specific network sections equipment and examine the network and the application protocol actions to detect malicious action. It has the ability to detect various kinds of actions of interest and is normally set up on boundary of networks, virtual private network servers, and wireless networks also remote access server.
3. Hybrid: it uses both host-based and network-based intrusion detection/intrusion prevention system concurrently.
4. Network Behaviour Analysis (NBA): investigates network traffic to recognize threats which produce abnormal traffic flows, like distributed denial of service attack, specific pattern of malware, and security policy abuse. These systems are usually set up to checks flows of internal networks, also checks flows between companies' internal network and external. (Mukhopadhyay et al, 2011).

3.1 Types intrusion detection/ intrusion prevention systems Techniques

There are several various techniques used by intrusion detection / intrusion prevention system to identify modification on the systems they check. These modifications are either external attacks or abuse by insider and of all these several techniques, four are mostly common which are Anomaly based, Signature based, Stateful protocol analysis, and Hybrid based. Presently intrusion detection/ intrusion detection prevention system applied hybrid techniques that combine different techniques to obtain a better identify and blockage capabilities are as follows: -

A. Anomaly Based Techniques: The anomaly based techniques is bothered with detecting activities which occurs to be anomalous with regards to usual system performance. A vast variety of methods which are data mining statistical modelling and hidden Mark or models have been studied as other methods to way the anomaly identify threat. Anomaly based technique includes the grouping of related data to the behaviour of real users for setting time frame and then use the statistical tests to the noticed behaviour is real user or threats. It is effective to identify attacks that are not been notice already, the main purpose for the use of this technique efficiently is to produce regulation like a pattern that it may lower the false alarm rate of violating security policy.

B. Signature based technique: The signature based techniques identify attack to specific a set of regulation which can be applied to determine that a given way is an attack, the signature base systems are efficient to obtain high level of accuracy as well as reduce number of false positives in detecting attack or threat small difference in known attacks can alter the investigation when the identify system is improperly set up. (Modi et al 2013). Hence, signature based techniques fails to identify strange attacks either change of known attacks. It is simple to maintain and updating pre-setup regulations.

C. State protocol Analysis based technique: it functions as equating obtained profile to the expected performance against the noticed performance of the obtained protocol profiles which creates as well accomplish by merchants, not like signature base technique that only equates noticed performance against a list, stateful protocol analysis have good knowledge protocols behaviour as well as usages will compatible/perform. The good knowledge/ investigation places very demanding overhead upon the system. Stateful protocol analysis combines and supports different intrusion detection/intrusion prevention system techniques strongly that lead to the emerging of hybrid techniques. Stateful protocol analysis good knowledge of how protocol will performance is applied as foundation for creating intrusion detection/ intrusion prevention system which good online traffic performance and are efficient in safe guarding websites. It is simple to bypass by intruders which follow and stay inside the acceptable performance of protocol. Therefore stateful protocol analysis techniques as well as methods has gradually been used and combine to different techniques over the past year, which led to the decrease use of intrusion detection/ intrusion prevention system that apply only stateful protocol analysis technique.

D. Hybrid based technique: the Hybrid based techniques use the merging of two or more various techniques. The outcome is more excellent because the techniques actually shared resources that makes them stronger when operating as a merged techniques. (Weng, Vespa and Soewito, 2011). Introducing the first hybrid intrusion detection system which gives a guideline depend on intrusion detection Message Exchange format (IDMEF), also the IETF standard which supports various sensors to exchange information, (Weng, Vespa and Soewito, 2011). The hybrid intrusion detection system of group-depended wireless sensors networks were suggested to function as dividing the identification into two, at a starting to applied anomaly depended model to identify intrusion attack, different model for the hybrid technique was introduced depend on the pattern of how human immune system functions.(Kenneth and Anil, 2007). The introduced system is depended upon rule of human immune system, which applies hybrid design that used both anomaly as well abuse identifying methods, (Kenneth and Anil, 2007) figure 1. Display common hybrid base techniques which has three different techniques that are merged. The monitored environment is examined by the start techniques and go to the behind one also to the one at the end, which make an excellent system.

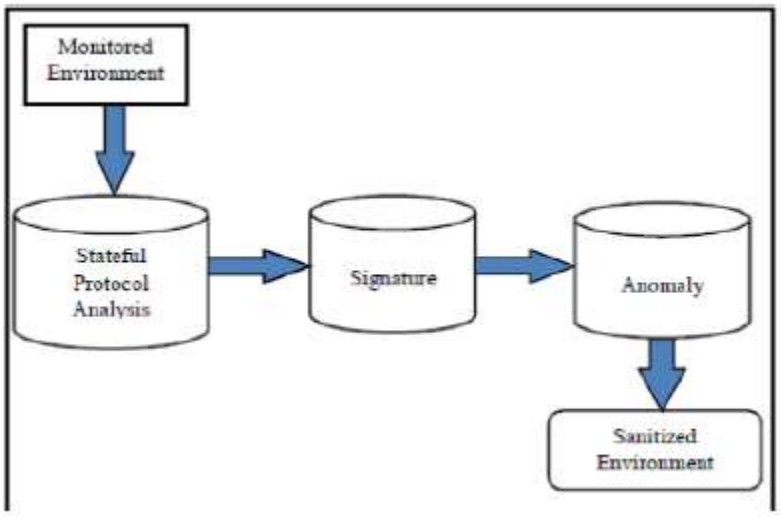

Figure1. Hybrid based methodology architecture. (Mudzingwa and Agrawal (2012))

3.2 **Advantages and disadvantages of intrusion detection/intrusion prevention system techniques.**

The following are the advantages and disadvantages of intrusion detection/intrusion prevention system techniques (Modi et al, 2013).

3.2.1 Signature based techniques

(i) Advantages of Signature based technique are:

(a) It detect intrusion by comparing captured methods and that of the preconfigured knowledge base.
(b) High identification of precision for already familiar attacks.
(c) Little computational expense

(ii) Disadvantages of signature techniques.
(a) It is not able to identify brand-new or change of familiar attacks
(b) Increase false alarm percentage for unfamiliar attacks.

3.2.2 Anomaly based technique.
(i) Advantages of Anomaly based technique
(a)It applied statistical test on accumulated behaviour to detect security violation or attacks.
(b)It reduce the false alarm percentage for unfamiliar attacks
(ii) Disadvantages of Anomaly base techniques
(a)It demanded plenty of time to detect attack
(b)Identify accurately is depended on quantity of gathered behaviour or characteristics

3.2.3 ANN based technique
(i) Advantages of ANN based techniques
(a)Grouping of unstructured network packet effectively
(b)Several unknown layers in ANN increases effectively on grouping.
(ii) Disadvantage of ANN based techniques
(a)Plenty of time is needed and several samples training phase

3.2.4 Hybrid based technique
(i) Advantage of Hybrid based technique
(a)It is more effective method to group rules accurately.
(ii)Disadvantage of Hybrid based technique
(a)Increase computational expenses.

4.0 Comparative analysis of intrusion detection/ intrusion prevention systems characteristics
It is based on technology layout, detection method, time of detection and data which are described as follows (Patel et al 2013).

4.1 Technology Layout:
(a) Wired: the wired networks are faster as well as little expense whereas the wired networks massively based on structure platform and very difficult to set up.
(b) Wireless: the wireless networks gives broad coverage and limitless access that expose to attack, the wireless is scalable as well as not depended on structure, also the usage of energy is low in mobile agent. Whereas the attacks which might be carry out on a wired network, the wireless itself required protection.

4.2 Time of detection:
(i) Real-time: it surpasses the development of attacks identify and stop it.
(ii) Non Real-time: it can cover up weakness of security networks related with vulnerable to different kinds of attacks which difficult to identify by general pattern of audit track examination and it possess must capabilities to supply prove of data forensic also acquire little resource usages. Whereas the Real-time identify is not able to manage encrypted packets, therefore it is not able to supply important information that needed for intrusion detection; source detection is obtained depended upon network address of the packet. Hence the source address can be spoofed and it becomes difficult to trace reaction to attacks; also it is very difficult as supply real time reactions to stop attacks on checks damages.

4.3 Data
(i) Distributed: the distributed data employ the traffic information of different roots in the method of data to examine the security situation of its own located network.
(ii) Central: it is the checking, identifying, and reaction events are been managed precisely by the central console. While the data movement among host monitors and the director agent will produce importantly increase network traffic overhead. The system applies the information majorly acquired from the packets on the network. Hence, data travels through more lengthy route from their roots to the intrusion system, and in the operation it might be damage or changed by an intruder that can lead to missed activities (Kerschbaum et al

2002); also it is possible for attacker to change or disable the configuration of programs running on the system which the intrusion detection/intrusion prevention system become not useful or undependable.

5. CONCLUSION

The comparative analysis of the Intrusion detection/Intrusion prevention system presented in this paper, examined the threat to confidential integrity and availability in information system whereby components of intrusion detection systems / intrusion preventive systems and their functionalities, type of intrusion detection/intrusion preventive systems, types of intrusion detection/intrusion preventive systems techniques, advantages and disadvantages of intrusion detection/intrusion preventive systems techniques and comparatives analysis of intrusion detection/intrusion preventive systems characteristics have been considered.

The intrusion detection systems limitation of not be able to preventive occurrence of future attack or preventive measure lead to intrusion preventive systems which have all the capabilities of intrusion detection systems, but because of the advantages and disadvantages that related to the types and techniques used in intrusion detection/intrusion preventive systems, a particular one not can withstand and protect information systems or computer network security from attack. Therefore, combination of four these intrusion detection/ intrusion preventive systems techniques are mostly used in market currently to ensure protection of CIA.

REFERENCE

1. Brown, D.J, Suckow, B. and Wang, T.(2002), A Survey of Intrusion Detection Systems, University of California, California, CA, available at: cseweb.ucsd.edu/classes/fao1/cse22/projects/group10.pdf.(Accessed: 25 November 2013).
2. Faysel M. A. and Haque S. S. (2010). 'Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention *Systems' IJCSNS International Journal of Computer Science and Network Security*, VOL.10 No.7, July 2010, Google scholar[Online].www.googlescholar.com.(Accessed: 25 October 2013).
3. Kerschbaum, F. Spafford, E.H. and Zamboni, D. (2002). Using internal sensors and embedded detectors for intrusion detection. Journal of Computer Security 2002; 10:23-70
4. Kenneth, L.I. and Anil, S. (2007). "*A Methodology for Designing Accurate Anomaly Detection Systems*" 4th international IFIPACM Latin American conference on Networking LANC O7 2007, 139.
5. Liao, H., Lin, C.R., Lin, Y., and Tung, K., (2013). 'Intrusion detection system: A comprehensive review'. *Journal of Network and Computer Applications* 36, 16-14, ELSEVIER [Online].DOI.10.1016/j.jnca.2012.09.004. (Accessed: 24 October 2013).
6. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., and Rajarajan, M., (2013).'A survey of intrusion detection techniques in Cloud.' *Journal of Network and Computer Applications*, 36 (2013) 42–57 Elsevier [Online].DOI.10.1016/j.jnca.2012.05.003 (Accessed: 29 October 2013).
7. Mukhopadhyay, I. Chakraborty, M., and Chakrabarti, S., (2011). 'A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems'. *Journal of Information Security*, 2, 28-38. SciRes. [Online]. DOI:10.4236/jis.2011.21003 (Accessed: 24 October 2013).
8. Mudzinggwa, D. and Agrawal, D. (2012) A study of methodologies used in Intrusion Detection and Prevention Systems IEEE, 9/12 IEEE Xplore [Online]. DOI: 978-1-4673-1375(Accessed: 27 November 2013).
9. Nalavade, K.C. and Meshram, B.B.(2011) 'Comparative Study of IDS and IPS' *BIOINFO Computer Engineering*, Volume 1, Issue 1, 2011, pp-01-04 .BIOINFO[online] http://www.bioinfo.in. (Accessed: 24 October 2013).
10. Patel, A., Taghavi, M., Bakhtiyari, K., and Junior, J.C., (2013). 'An intrusion detection and prevention system in cloud computing: A systematic review' *Journal of Network and Computer Applications*, 36, 25-41. Elsevier [Online].DOI.10.1016/j.jnca.2012.08.007. (Accessed: 29 October 2013).
11. Patel, A., Qassim, Q., and Wills, C., (2010). 'A survey of intrusion detection and prevention systems' *Information Management & Computer Security* Vol. 18 No. 4, 2010 pp. 277-290. Emerald [Online]
12. DOI 10.1108/09685221011079199(Accessed: 25 October 2013).
13. Weng, N., Vespa, L. and Soewito, B.(2011). "Deep packet pre-filtering and finite state encoding for adaptive intrusion detection system" Computer Networks 55-1648-1661.