IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. V (Jul – Aug. 2014), PP 99-101
www.iosrjournals.org

Multi-Level Based Hybridized Intrusion Detection and Prevention System

Okunade Oluwasogo Adekunle
[1]*School of Science and Technology, National Open University of Nigeria, 14/16, Ahmadu Bello Way, Victoria Island, Lagos, Nigeria.*

Abstract: *Global spread of Information Technologyincreases security challenges; over intrusion detection system against sophisticated attacks. This has become of paramount importance since single mode intrusion detection systems have a lot of difficulties in protecting Network from sophisticated attackers. However, this paper propose a Multi-Level Based Hybridized Intrusion Detection System whereby the incoming packets will be examinedfor attacks at two layers; both at Network level as Network Intrusion Detection (NID) and further double check those that escape through the initial test at the second level using Bayes' theorem at Host level as Host based Intrusion Detection (HID). This will help to prevent against intrusion, minimize false alarms and maximize the numbers of detected bad events. It handle masses of information (often in real-time) so as to report the abnormal use of networks and computer systems in a real time before it get out of hand.*

Keywords: *Intrusion, Hybridized, Packet, IntrusionDetection and prevention System, Network Intrusion Detection, Host basedIntrusion Detection, Multi-Level Based Hybridized Intrusion Detection System (MHIDS).*

I. Introduction

An intrusion is defined to be a violation of thesecurity policy of the system; intrusion detectionthus refers to the mechanisms that are developedto detect violations of system security policy [1].Intrusion detection system (IDS)dynamically monitors the events taking place in a system,and decides whether these events are symptomatic of anattack or constitute a legitimate use of the system [2] in [3].Single mode intrusion detection systems are not adequate to protect Network from Inside and Outside attackers; Single base IDS tools are notorious for false positives. However detecting sophisticated threats like "low and slow" attacks and other stealthy malicious activity is very difficult for the single perimeter based IDS to be able to detect.According to[4]network IDS monitor network traffic canraise an alert on suspected intrusion packets or act on those packets such as blocking them or resetting concernedconnections. Intrusion detection systems (IDS) dynamically monitors the events taking place in a system, and decidewhether these events are symptomatic of anattack or constitute a legitimate use of the system [5] in [3]. Denials of Service (Dos) attacks are probablythe nastiest, and most difficult to address. These are most horrible, because they are very easy to launch, difficult (sometimes impossible) to track, and it is not easy to refuse the requests of the attacker. Certain information (Such as personal record, company information, credit card details and others) would cause damage once inthe hand of a competitor, an enemy or the public. In this case, it is possible that a normal users account on the machine can be enough to cause damage, while many of the perpetrators of this sort of break-in can be merely thrill-seekers interested in nothing or more malicious sort of break-in[6].

Therefore IDS is needed with capability of detecting inside and outside, known and unknown attacks with low false alarm rate for effective Intrusion Detection.Networkis any set of interlinking lines resembling a net. A computer Network is simply a system of interconnected computers in order to share resources; exchange files, or allows electronic communications.This consists of a collection of computers, printers and other equipment that is connected together so that they can communicate with each other. However computers on the networks are vulnerable to Intrusion due to network wider open and expansion. Both wired and wireless Networksarealso vulnerable to Intrusion.No open computer network is immune from intrusions: only wireless Ad hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of clear line of defense [7]. The suggestion that Anomaly models for wired network cannot be used in wireless environment becausewired network traffic monitoring is usually done at switches, routers and gateway, while Had hoc network for instancedoes not have such traffic concentration points where the IDS can collect and audit data for the entire network.

Wireless sensor networkaregenerally positioned to consist of a large numbers of inexpensive nodes reporting their data to a central and more capable sink node; using multihop transmission. They are vulnerable to several attacks due to their deployment in an open and unprotected environment [8]. Itmakes use of a sensor node which is a tiny and simple device with limited computational capability and broadcast power. Itis assumed that sensors will be equipped with non-rechargeable batteries and will be left unattended after deployment.

However, current and foreseeable future technology has put severe restraints on energy resources of sensor devices. Because, long term operation of nodes with limited battery energy is the main design bottleneck of sensor networks. Therefore, sensor network protocols haveto be designed to operate with minimum resource utilization. Security solutions for sensor networks also have to be designed with the limited computational power, limited memory and limited battery life of sensor nodes in mind [9].

Two main techniques for security solution are;Intrusion prevention mechanisms, such as authentication, key management, security, routing protocols, and so on, can stop the deceptive attacks launched by external attackers, but it is difficult to confront the DOS attacks which have stronger concealment and destructive power and difficult to confront the deceptive attacks launched by captured node. These attacks must be found and handled through intrusion detection mechanism [9] that can detect and block attacks before damage has been done. It is a set of actions that determine, and report unauthorized activities. It detects the violation of confidentiality, integrity and availability [8]. AndIntrusion Detection technique this is to identify theattacks basedon the systems behavior. Two different kinds of detection technique are Anomaly based, which observed the activities that deviate significantly from the established normal usage profiles as anomalies (likely possible intrusion).This require not prior knowledge of intrusion to detect new intrusions, but may not be able to describe what the attack is and may have high rate of false positive rateand Signature based using pattern of well-known attacks or weak spots of the system to match and identify known intrusions. It can accurately and efficiently detect instances of known attacks but lack of ability to detect truly innovative (new) attacks[8]. By knowing the paths of vulnerability through our networks, we can reduce the impact of attacks. Traditional tools for network vulnerability assessment simply scan individual machines on a network and report their known vulnerabilities.

Information Systems and Networks are subject to electronic attacks. Attempts to breach information security are rising every day, along with the availability of the Vulnerability Assessment tools that are widely available on the Internet, for free, as well as for a commercial use [10].Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting intrusion attempts. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. IDS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed. Intrusion detection and prevention systems (IDPS) technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed: We have network based (NIDS) and host based (HIDS) intrusion detection system:Network Intrusion Detection and Prevention system works on analyzing the packets coming and going through the interface, runs at the gateway of a network, captures and examines network packets that go through the network hardware interface.The remainder of this paper is organized as follows; Section 2 introduces the framework for the Multi-Level Based Hybridized Intrusion Detection System (MHIDS). Section 3 describes the result of the frame work. Section 4 discusses the result gotten from the given framework in Section 2. Finally, important conclusion is discussed in Section 4.

II. Methodology

In this paper we are concerned with combination of two different techniques (Anomaly detection using signature at the Network level as Network Intrusion Detection (NID) and content filter using Bayes’ theorem at Host level as Host based Intrusion Detection (HID)) forthe process and implementation ofIDS. However this will be able to detect sophisticated threats like "low and slow" attacks and other stealthy malicious activity that a single perimeter based IDS on its own will not be able to detect.

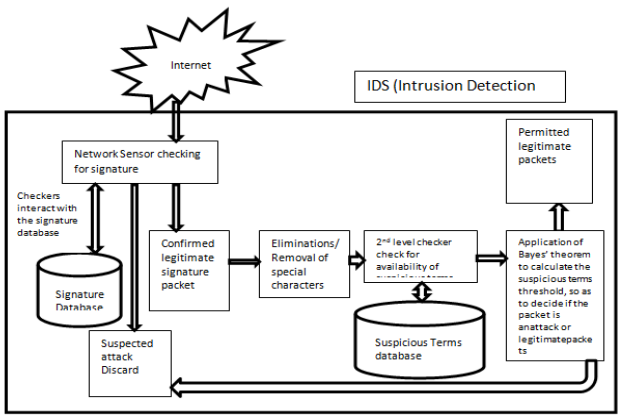

Figure2.1: Multi-Level Based Hybridized Intrusion Detection System Architecture
Source: Field work

IDSat the network base will monitor and analyze the traffic passing through its networksegment to detect intrusion attempts. Itdetermines if packet flow matches with a known signature. Havingcompared the packet signature with the known database signature, those confirmed to be attack will be blocked and those confirmed legitimate will be passed to the next level of checking. According to [11]firstly,removethe unwanted special characters used to manipulate the suspicious terms such as; $, /, \, |, =, !, @, #, %, ^, &, *, (,), <, >, ?, :, ”, ’, {, [, },] used to foil the filtersto prevent them from being identified. Having done this, the content checker will then check the entire content byapplying Bayes’ theorem as follow:

$$p(a,b,c...z)=\frac{a*b*c*.....*z}{a*b*c*.....*z+[(1-a)*(1-b)*(1-c)*.....*(1-z)]}$$

Where:

a = is the first packet token to be discovered as suspicious token in the Suspicious database,

b= is the second packet token to be discovered as suspicious token in the Suspicious database,

c= is the third packet token to be discovered as suspicious token in the Suspicious database,

z = which is the last packet token to be discovered as suspicious token in the Suspicious database.

To calculate if the packet is an attack or legitimate packed based on the available number of suspicious term discovered within the content of the packed. If result of the Bayes’ theory get to a particular thresholdofP(a,b,c,…..,z) >= 0.5 the packet will be classified as an attack and will be block, otherwise it will be permitted as the legitimate packed.

III. Results And Discussion

Multi-Level Based Hybridized Intrusion Detection System (MHIDS) is highly effective at combating incoming attacks; at both Network and Host based level to double check the packet for attack at two layers. However, there will be double assurance of the IDS outcome and this will help to checkmate the level of intrusion and classified the packets to be legitimate or attack based on the result/outcome of the analysis.

IV. Summary And Conclusion

Invoked MHIDS gives more extensive forensic investigation, when configured it minimize false alarms, and maximize the number of detected bad events. It handle masses of information (often in real-time) so as to report the abnormal use of networks and computer systems in a real time.

References

[1] C. Srilatha, A. Ajith & P. T. Johnson, Feature deduction and ensemble design of intrusion detection systems, Elsevier, Computers & Security (2004), www.elsevier.com/locate/cose

[2] H. Debar, M. Dacier and A. Wespi, ”Towards a taxonomyof intrusion-detection systems” Computer Networks, vol. 31,pg. 805-822, 1999.

[3] F. E. Heba, D. Ashraf, E. H. Abouland A. Ajith, Principle Components Analysis and Support Vector Machinebased Intrusion Detection System, 10th International Conference on Intelligent Systems Design and Applications, 978-1-4244-8136-1/10/IEEE, 2019 Pg 363-367

[4] K. S. Sandeep, C. Nishant and S. Pragya, Concept and Proposed Architecture of Hybrid Intrusion Detection System using Data Mining, International Journal of Engineering and Advanced Technology (IJEAT). ISSN: 2249 – 8958, 2(5), 2013

[5] H. Deber, M. Dacier and A. Wespi., Towards a Taxonomy of Intrusion Detection Systems, Computer Networks, Vol 31 1999 pg 805-822

[6] A. Shaik,K.N.Rao, J. A. Chandulal, Intrusion Detection System Methodologies Based on DataAnalysis, International Journal of Computer Applications (0975 – 8887). 5(2), 2010 Pg. 10-20

[7] Z. Yongguang and L. Wenke, Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of the Sixth Annual International Conference onMobile Computing and Networking (MobiCom’2000), pg.6–11, Boston, Massachussetts

[8] I. M. Safiqul and S. AshiqurRahman, Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches. International Journal of Advanced Science and Technology (36), 2011

[9] Z. Han and R. Wang, Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model, International Conference on SolidState Devices and Materials Science, PublishedbyElsevierB.V.Selection and/or peer-review under responsibility of Garry Lee doi:10.1016/j.phpro.2012.03.352,

[10] SANS InstituteInfoSec Reading Room, SANS Institute 2001,www.sans.org/reading-room/click/528

[11] O. A. Okunade, Word Stemming/Hashing Algorithm for Mail Classification, LAP LAMBERT Academic Publishing Gmbh& Co. KG. Heinrich-Bocking-Str. 6-8, 66121 Saarbrucken, Germany. ISBN: 978-3-8473-0672-6, 2011