Covenant Journal of Informatics & Communication Technology. Vol. 7 No. 1, June, 2019
ISSN: p2354-3566 e 2354-3507 DOI: 10.20370/xtjk-4b94

An Open Access Journal Available Online

Hybridized Intrusion Detection and Prevention System Using Static IP Address

Oluwasogo Adekunle Okunade

Department of Computer Science, Faculty of Sciences, National Open University of Nigeria,
Abuja, Nigeria.
aokunade@noun.edu.ng

Received: 3.12.2018 Accepted: 16.04.2019 Date of Publication: June, 2019

Abstract—Internet growth and constant increase in traffic volume, resulted into various misuse and attacks on the internet, that increases security challenges over intrusion detection and prevention system against sophisticated attacks. This has become paramount importance since single mode intrusion detection systems have a lot of difficulties in protecting system and network from sophisticated attacks. However, this paper propose hybridized intrusion detection and prevention system using static IP address whereby the incoming packets are examined for attacks at two layers, both at network level as network based intrusion detection and prevention system (NIDPS) and at host level as host based intrusion detection and prevention system (HIDPS) to further strength system and network security. This help to prevent against intrusion, minimize false positive and negative alert and maximize true positive and negative detection. This technique handled sufficient information in a real-time to account for irregular use of networks and computer systems in a real time.

Keywords/Index Terms— Security, Attack, Vulnerability, Network and filtering.

1. Introduction

Internetworking Protocol (IP) addresses are the unique numeric identifiers required of every devices connected to the Internet. It is a standard network layer protocol of the Internet architecture, that permitted communication within the various networks (Paulo & Joel, 2010). They are used for data routing across the internet. An IP address can be static (fixed) or dynamics (changes). Static IP addresses are specific IP addresses that are manually assigned by an administrator. Where dynamic IP addresses are not fixed but changes, automatically assigned by Dynamic Host Configuration Protocol (DHCP).

An intrusion is defined as violation of security policies that govern a particular system or network (Okunade, 2014). It is forcefully abuse or take advantage of someone's computer system or a network, with the intent of stealing personal information or reduce the functionality of a targeted system. This could be achieved through computer viruses, phishing, or other types of social engineering. Computer security is information security applied to computers and networks to monitor, control and prevent an unauthorized access to a system or a network, such as: hacking, Intrusion, data loss, data theft and data destruction, that are primarily internet security challenge (Jabez and Muthukumar, 2014 in Rajendran, Muthukumar and Nagarajan, 2015).

Intrusion Detection and prevention System IDPS is a network supervise or aware system, that primarily focused on identifying potential incidents. It is used to identify, examine, frustrate and report activities that are not consistent and tampering of data stored on the computer networks by unauthorized users. Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS) for it is configured to block any alleged anomalies without human interference. It is a real-time security detective and preventive system developed to discover violations of system security policy (Vani, 2016 and Srilatha, Ajith, & Johnson, 2004 and Dave, Trivedi & Mahadevia, 2013). It dynamically monitors the events taking place in a system, and recognize every symptom of attack (Debar, Dacier & Wespi, 1999 in Heba, Ashraf, Abouland & Ajith, 2018).

Single mode intrusion detection systems are not sufficient enough to safe guard dynamic level of today's network operations and activities due to the sophisticated means of attach that could be launch unaware. Single base IDS tools are notorious for false positives. However detecting sophisticated threats is very difficult for the single perimeter based IDS to be handle. According to Sandeep, Nishant and Pragya (2013) Network IDS monitor network traffic can raise an alert on suspected intrusion packets or act on those packets such as blocking and resetting concerned connections. It is a network monitor and alert system raises an alarm before the attack is being done and protects the system from various attacks (Ananthi and Balasubramanie, 2014 and Mehrnaz, Babak. and Iraj, 2018). An attack such as Denials of Service (Dos) are the most complex type of an attack to tackle, very easy to initiate and sometimes impossible to decline the requirements of the invader. However, an entry point of access security is highly required as an additional security support. Since the beginning stage research security focus that mostly lies in using statistical approaches and rule-based expert systems were not accurate, when encountering larger datasets according to (Manikopoulos and Papavassiliou, 2002 in Jabez and Muthukumar, 2015). Manu (2016) suggested that IDE can only be used as secondary wall of defense network security measure. As network growth and become complex, the IDE become weaker, as such, collaborative measure is highly required to strengthen the IDPS effectiveness. Remainder of this paper is organized as follows: Section 2 is the background of the work, Section 3 is the proposed algorithm and implementations, Section 4 describes the result derived from the given framework in Section 3. Finally, important conclusion is discussed in Section 5.

2. Background of the Work

2.1. Denial of Service (DoS) Attacks

DOS attacks is a strong destructive attack difficult to deal with (Nadiammai & Hemalatha, 2014). It slow or shut down the target to disrupt services and deny authorized users (Manu, 2016). These attacks must be found and handled using an effective intrusion detection mechanism to detect and obstruct the attacks before implementation (Han and Wang, 2012). Intrusion detection mechanism classify packets as either legitimate or malicious, having carefully examine the packet (Osanaiye, Cai, Choo, Dehghantanha, Xu, & Dlodlo, 2016).

2.2. Intrusion Detection System IDS

Intrusion Detection System IDS is a software that monitors network activities for abnormal detection or violation of system or network established policies. It was introduced to avoid security inaccuracy and false alarm rate (Shamshirband, Anuar, Kiah, Rohani, Petković, Misra and Khan, 2014). IDS consists of review data collection agent that gathered information on the observed system, for storage or decision making having analyzed the gathered information Muamer and Norrozila, 2012). It could be destructive, if vital information (Such as personal, company, credit card details and others) could get into the hand of an intruder. Meaning that it is achievable that normal user’s account on the machine can be adequate to cause damage (Shaik, Rao and Chandulal, 2010). According to Sonali, Madhuri, Jyoti, Sunanyna and Patil (2017) function of an IDPS is to offer protection to spread computing environments which are controlled and managed by a particular network. IDPS perform confidentiality as a function in the sense that authorized users are only allowed to access the information. Integrity which is the trustworthiness of information and data, consistency and availability of information only to the authorized users.

Therefore, IDS is highly required with the qualifications of identifying known and unknown attacks with little or no false negative or positive rate for effective intrusion detection. IDS is a collective tools, methods, and resources that help to identify and report intrusion in a system or network (Ismail, Salvatore & Ravi, 2013). Prevention of a system or network compromise of: confidentiality, availability and integrity of the system, data stored and control are the main function of an IDS (Alex, David and Aladdin, 2018). Network is any set of interconnecting lines in the form of a net. Computer network is therefore a system of interconnected computers in order to share resources; such as files exchange, or 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 expansion and openness both wired and wireless. Wireless Ad hoc network are particularly vulnerable due to their features of openness, vibrant changing topology, supportive algorithms, non centralized monitoring and management point and lack of defense (Yongguang and Wenke, 2000). Wired networks used anomaly detection methods that is not applicable to wireless network environment (Yassine, Abdellah, Youssef and Mohamed, 2015), due to the fact that wired network traffic had a concentrated points where the IDS gather and inspect data for the network, which is not applicable to wireless network (Safiqul and AshiqurRahman, 2011). High growth rate of wireless networks compared with traditional wired network is replacing traditional wired networks gradually due to their unique architecture and features (Abdulsalam, Tarek and Elhadi, 2014). Two different kinds of detection technique are:

1. Anomaly based IDS: This observe behaviour that are different from customary standard practice. This make use of statistical modeling to model anomaly detection component that has its bases as a reference and compare with actual parameters generated by the system or network under test (Vishwa & Salvatore, 2018 and Aljawarneha, Aldwairia & Yasina, 2017). It has high rate of false positive, it requires not previous knowledge of intrusion to detect new intrusions, as such it may not be able to illustrate the attack.

2. Signature based IDS: This makes used of blueprint of known attacks or a particular system weak spots to match and identify known intrusions. it is accurate and efficient in identify known attacks but inability to detect innovative (new) attacks (Safiqul et al, 2011).

2.3. Intrusion Detection and prevention System IDPS

IDPS is a set of actions that identify and reports abnormality activities such as violation of privacy, reliability and network or computer accessibility (Safiqul et al, 2011). It inspects all inbound/outbound network operation and identifies any non adopted policy patterns from any system or individual on an attempt to break the lay down policy (Syed, Gabriel, Matt & Jeremy, 2016). Intrusion detection and prevention systems (IDPS) are mainly alert on identifying possible incidents, logging information concerning the incidents and reporting intrusion attempts. Intrusion detection and prevention systems (IDPS) technologies are differentiated by the types of proceedings that they monitor and the deployed conduct: Network based Intrusion Detection and prevention System (NIDPS) this analyzes the incoming and outgoing packets through the interface. It runs at the gateway of a network, captures and examines network packets that go through the network hardware interface. And host based Intrusion Detection and Prevention System (HIDPS): analyzes the incoming and outgoing packets through the interface gateway of a host. It captures and examines host packets that go through the system interface**.**

Numbers of research works have investigated the challenges of intrusion detection and prevention system. Where most of their suggested solutions deal with either detection or prevention of basic single host base malicious detection and or prevention and basically dynamic IP address. Nadiammai et al. (2014) suggested the concept of data mining integrated with an IDS to identify hidden relevant data, for effective packet classification using EDADT algorithm, Hybrid IDS model, Semi-Supervised Approach and Varying HOPERAA Algorithm. Alex et al. (2018) suggested artificial neural network (ANN) architecture that give an average accuracy of 98%, and an average rate of less than 2% of false positive. Aljawarneha et al. (2017) proposed an Anomaly-based hybridized intrusion detection approach that consists of J48, Meta Pagging, RandomTree, REPTree, AdaBoostM1, DecisionStump and NaiveBayes classifiers to give an improved accurate result.

Shamshirband et al. (2014) introduced cooperative-based fuzzy artificial immune system (Co-FAIS) where network agents work with one another to discover sensor's abnormality of in terms of context antigen value (CAV) to update fuzzy activation threshold for security response. To reinforced to defend against an incoming DDoS attack. Vishwa et al. (2018) come up with a wireless Sensor Network (WSN) security. Using an immune theory technique, designed based on the functions of various immune cells using energy, volume and frequency of data transfer as a basis for IDS design in WSNs to predicted different forms of attack for accurate detection of WSN attacks. Gupta, Dhawale & Misra (2016) called for dimensional security remedies to overcome challenges of insecurity in today's mobile communication system. They suggested lowest cluster identity and highest connectivity within the nodes as the cluster head and did distance based parameter cluster head selection to gives efficient way for detecting the malicious node.

3. Proposed Algorithm and Implementations

3.1. Methodology

This paper presents a Host based Intrusion Detection and Prevention (HIDP) Security System for an organizational security control, as an additional support to Network based Intrusion Detection and Prevention System (NIDPS), to further strengthen the organisation security measure. It enforced combinations of User ID, User type, system MAC Address and assigned static IP address (USER ID + USERTYPE + MAC ADDRESS + IP ADDRESS) from network users, at Host level as Host based Intrusion Detection and prevention system (HIDPS). In order to gain access to an organisational system or network. Before an access can be granted/ permitted in an organizational network system.

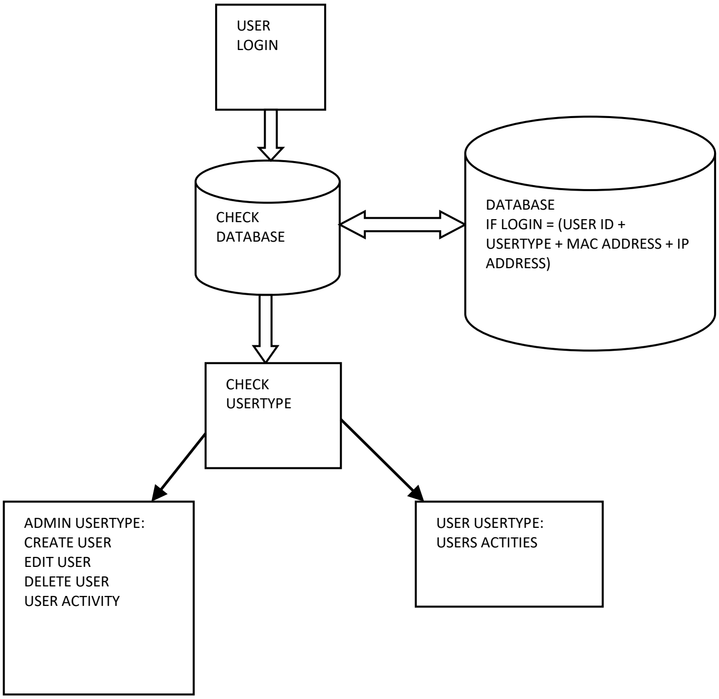

Figure1: Hybridized Intrusion Detection and Prevention System Using Static IP Address, Field Work

Security algorithm in figure 1 at the point of login compulsorily demand from user to supply the following login parameters: User ID, User type, system MAC address and assigned static IP address (USER ID + USERTYPE + MAC ADDRESS + IP ADDRESS). It then compare supplied parameters against the user supplied information at the point of registration stored in the database. if matched, user will be granted access, level of access granted user will be determined based on the user type. If ordinary user the level of access granted will be minimal, then further network security level will be implemented. But if user type is Administrator, user will be granted maximum access to operate on the system, before facing advanced level of network security. Otherwise, if user supplied wrong information, access is denied. Algorithm ensure total compliance of requested information from the user, before granting access to the legitimate users alone.

4. Results and Discussion

4.1. Results

This show result of implementation of Algorithm in figure 1.

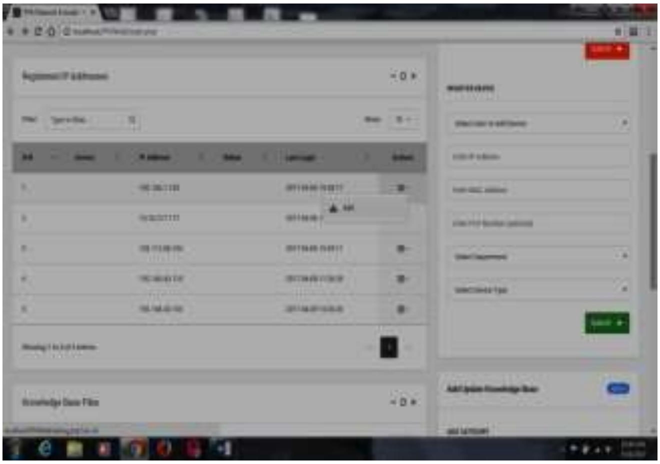

Figure 2: Registered IP Address Interface

This is an interface figure 2 where administrator register users, by assigning user with login information such as (User ID, User type, system MAC Address and assigned static IP address) that are compulsorily needed to login to the system or network.

Figure 3: Login Interface

This is login interface figure 3 where user supply the login parameter in order to gain access to the system or network.

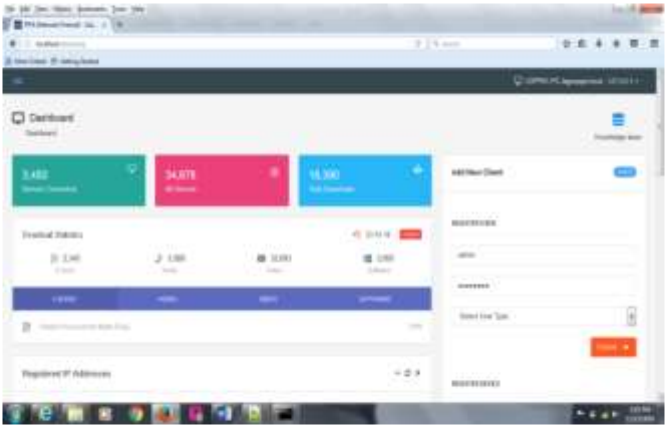

Figure 4: Dashboard Interface

Figure 4 is a dashboard interface, it is home page for users to supply their correct login parameters. To login to the system and then network to perform available choices of operation. User type (such as: user and administrator). control and determine level of operation a user can perform. The checking at this level is the initial level of security that further required other additional levels of security checking to ensure effective user /security affirmation.

4.2. Discussion

Hybridized Intrusion Detection and Prevention System Using Static IP Address is highly effective at preventing unauthorized access to a system or network. At point of user login interface, to ensure user legitimacy before granting access. Result of the tested algorithm show that algorithm prevent access to user without correct required information supplied (such as correct: User ID, User type, system MAC Address and assigned static IP address) access denied is replied instead, at the host level. This prevent user from qualify for further level of network based security control. Both host and network based security levels are rigorously checked to guarantee system and network security safety against intrusion.

Hybridized based security system advantages cannot be over-emphasized in these modern days technology breakthroughs. Addition of a host based hybridized intrusion detection and prevention system, ensure system and network security reliability, to enforce minimal false positive and negative alert.

5. Conclusion

This algorithm strictly enforced supplying of all mandatory required login parameters (User ID, User type, system MAC address and assigned static IP address) before granting access to users, otherwise access is being denied. If any of the require information is missing or not properly supplied. The algorithm was tested and function efficiently and effectively accordingly. This served as an additional security measure for intrusion detection and prevention system.

References

Abdulsalam, B., Tarek, S. and Elhadi, S. (2014). Implementation of A3ACKs intrusion detection system under various mobility speeds. 5th International Conference on Ambient Systems, Networks and Technologies. www.sciencedirect.com

Alex, S., David, D. and Aladdin, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express 4. Pp. 95–99. www.elsevier.com/locate/icte

Aljawarneha, S., Aldwairia, M. and Yasina, M. B. (2017). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science. www.elsevier.com

Ananthi, P. and Balasubramanie, P. (2014). An Adaptive Hybrid Multi-level Intelligent Intrusion Detection System for Network Security. Research Journal of Applied Sciences, Engineering and Technology 7(16)

Ismail, B., Salvatore, D. M. and Ravi, S. (2013). A Survey of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials. www.researchgate.net

Dave, S., Trivedi, B. and Mahadevia, J. (2013). Efficacy of Attack Detection Capability of IDPS Based On Its Deployment in Wired and Wireless Environment. International Journal of Network Security & Its Applications (IJNSA), Vol.5(2)

Debar, H., Dacier, M. and Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer Networks. vol. 31, pp. 805-822.

Gupta, D., Dhawale, C. and Misra, S. (2016). A Cooperative approach for Malicious Node Detection in impromptu Wireless Networks.International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). IEEE

Han, Z. and Wang, R. (2012). Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model, International Conference on Solid State Devices and Materials Science. Published by Elsevier

Heba, F. E., Ashraf, D., Abouland, E. H. and Ajith, A. (2018). Principle Components Analysis and Support Vector Machine based Intrusion Detection System 10th International Conference on Intelligent Systems Design and Applications. IEEE. Pp 363-367

Jabez, J. and Muthukumar, B. (2015).Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach. International Conference on Intelligent Computing, Communication & Convergence. Procedia Computer Science Vol. 48, pp. 338 – 346. www.sciencedirect.com

Jabez, J. and Muthukumar, B. (2014). Intrusion Detection System: Time Probability Method and Hyperbolic Hopfield Neural Network. Journal of Theoretical and Applied Information Technology. 67(1), pp 65-77.

Manikopoulos, C. and Papavassiliou, S. (2002). Network intrusion and fault detection: A statistical anomaly approach. IEEE Communications Magazine. 40(10), pp. 76–82.

Manu, B. (2016). A Survey on Secure Network: Intrusion Detection & Prevention Approaches. American Journal of Information Systems, Vol. 4(3). http://pubs.sciepub.com/ajis/4/3/2. Science and Education Publishing

Mehrnaz, M., Babak, S. and Iraj, M. (2018). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University –Computer and Information Sciences. www.sciencedirect.com.

Muamer, N. M. and Norrozila, S. (2012). Intrusion Detection System Based on SVM for WLAN Published by Elsevier Ltd. Procedia Technology Vol. 1, pp. 313 – 317. www.sciencedirect.com

Nadiammai, G.V. and Hemalatha, M. (2014). Effective approach toward Intrusion Detection System using data mining techniques. 15, pp. 37-50 www.elsevier.com/locate/eij, www.sciencedirect.com

Okunade, O. A. (2014). Multi-Level Based Hybridized Intrusion Detection and Prevention System. IOSR Journal of Computer Engineering (IOSR-JCE) 16(4), pp. 99-101 www.iosrjournals.org www.iosrjournals.org.

Osanaiye, O., Cai, H., Choo, K. R., Dehghantanha, A., Xu, Z. and Dlodlo, M. (2016). Ensemble-Based Multi-Filter Feature Selection Method for DDoS Detection in Cloud Computing. EURASIP Journal on Wireless Communications & Networking. Pp1-10

Paulo, A. C. and Joel, J. P. (2010). Internet Protocol over Wireless Sensor Networks, from Myth to Reality. Journal of Communications, 5(3), pp. 189-196

Rajendran, P. K, Muthukumar, B. and Nagarajan, G. (2015). Hybrid Intrusion Detection System for Private Cloud: A Systematic Approach. International Conference on Intelligent Computing, Communication & Convergence. Pp. 325 – 329. www.sciencedirect.com

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

Sandeep, K. S., Nishant, C. and Pragya, S. (2013). Concept and Proposed Architecture of Hybrid Intrusion Detection System using Data Mining, International Journal of Engineering and Advanced Technology (IJEAT). 2(5).

Shamshirband, S, Anuar, N.B., Kiah, M.L.M., Rohani, V. A., Petković, D., Misra, S. and Khan, A. N. (2014). Cooperative Fuzzy Artificial Immune System for Detecting Intrusion in Wireless Sensor Networks. Journal of Network and Computer Applications (Elsevier), 2014, Vol. 42, pp. 102–117. www.elsevier.com

Shaik, A., Rao, K. N. and Chandulal, J. A. (2010). Intrusion Detection System Methodologies

Based on DataAnalysis, International Journal of Computer Applications. 5(2), pp.10-20

Sonali, N., Madhuri A. D., Jyoti, B., Sunanyna S., Patil, D.Y. (2017). A Comparative Study of

Intrusion Detection System tools and Techniques. International Journal of Innovative Research in Computer and Communication Engineering. 5(8). www.ijircce.com

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

Syed, R., Gabriel,L., Matt, G. and Jeremy, S. (2016). Advocating for Hybrid Intrusion Detection Prevention System and Framework Improvement. Published by Elsevier B.V. Procedia Computer Science Vol. 95, pp. 369 – 374. www.sciencedirect.com

Vani, A. H. (2016). Intrusion Detection: A Survey. International Journal of Innovative Research in Computerand Communication Engineering. Vol. 4(2). www.ijircce.com

Yassine, M., Abdellah, E., Youssef, Q. and Mohamed, M. (2015). A Global Hybrid Intrusion Detection System for Wireless Sensor Networks. The 5th International Symposium on Frontiers in Ambient and Mobile Systems. Published by Elsevier B.V. Computer Science 52, pp. 1047 – 1052. www.sciencedirect.com.

Vishwa, T. A, and Salvatore, D. M. (2018). A Multi-Level Intrusion Detection System for Wireless Sensor Networks based on Immune Theory. IEEE

Yongguang, Z. and Wenke, L. (2000). Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking. pp.6–11