DEVELOPMENT OF A NETWORK SECURITY SYSTEM USING INTRUSION DETECTION AND LOG MANAGEMENT

I J. MGBEAFULIKE [(1)], E. O CHUKWUOGO. [(2] ANDEZEANYEJI P.C [(3)]

[1,3]Department of Computer Science Chukwuemeka Odumegwu Ojukwu University, Uli Email: ike.mgbeafulike@gmail.com
[2]Anambra Internal Revenue Service No.1 Esther Obiakor Avenue, Agu-awka Email: oquichuks@gmail.com

ABSTRACT
The rapid increase in computer, mobile applications and wireless networks has globally changed the features of network security. A series of Internet attack and fraudulent acts on companies and individual network have shown us that open computer networks have no immunity from intrusions. The traditional way of protecting computer networks, such as firewalls and software encryption are insufficient and ineffective. Protecting computer and network security are critical issues. The malicious nodes create a problem in the network. This malicious nodes acts as selfishness, It can use the resources of other nodes and preserve the resources of its own. After analyzing and quantifying the network information security elements confidentiality, integrity and availability, this paper provides solution to those insecurities. Since the techniques developed on fixed wired networks to detect intruders have been rendered inapplicable in this new environment, the need for ways and methods to develop new architecture and mechanisms to protect wireless networks is important. Many problems small companies are facing due to intruders and attackers are also as a result of poor network security. Basically, the vulnerabilities and mitigation this journal examines will be very useful in the underdeveloped and developing nations.

Keywords: Network, Security, Intrusion, Intrusion detection, Log

1. INTRODUCTION

Several possible fields of endeavor come to mind within this broad topic, and each is worthy of a lengthy article. To begin, network security can be said to be any activity designed to protect the usability and integrity of your network and data. It is also the generic name for the collection of tools designed to protect data during their transmission. An effective network security manages access to the network, targeting a variety of threats and stopping them from entering or spreading in the network. It consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. The security may include identification, authentication and authorization, and surveillance camera to protect integrity, availability, accountability, and authenticity of computer hardware or network equipment. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. In fact, viewed from this perspective, network security is a subset of computer security. A good network security protects a network in a manner that is consistent with its purpose, in other words, they have to be designed to fit the needs of their organization's network and not anyone else's. The problem most network faces are network insecurity. This is sometimes more than what people always thought it to be, malware, virus, Trojan, hackers. It could be caused by unintentional human error and could be compromised by human nature as well. A common network security problem most organizations are facing sometimes has to do with the company's employees and their various errors they make. The problem of piracy is another common network problem. This is a situation

where intellectual properties are compromised although there are technical mechanisms that aid in enforcing copyright laws to tackle this problem. It is not only humans that can cause problem to network security, problems can also be caused by natural forces like fire breakouts, earthquakes, floods lightning etc. The objective of this study is to develop a network security system using intrusion detection and log management.

2. LITERATURE REVIEW

Network attacks have been discovered to be as varied as the system that they attempt to penetrate. Attacks are known to either be intentional or unintentional and technically competent intruders have been interested in targeting the protocols used for secure communication between networking devices, (Reed 2003). According to Dr. Michael E. Whitman, CISM, CISSP, and the author of the textbook "*Principals of Information Security*, "Humans make mistakes; sometimes that is due to inexperience or improper training, and sometimes it is because an incorrect assumption was reached. But regardless of the reason and the lack of malicious intent, something as simple as a keyboarding error has the potential to cause a worldwide Internet outage", (Whitman and Mattord 2012). A data mining approach to network intrusion detection (Roesch 1999) provides an opportunity to learn the behaviors of network users by mining the data trails of their activities. Though recent research e.g., Clustering (Zhong et al 2007), had investigated data mining for intrusion detection, significant challenges are unexplored. This involves intrusion detection models for wireless networks not requiring hard-to-get training data in wired network environment, as well as intrusion detection (Buchtala et al 2005) that has no prior knowledge of relationships between attack types and attributes of the network audit data (Deckerd 2006).

2.1. Types of Intrusions in Network: In this section, important classes of intrusion that commonly affect network are described.

- **Denial of Service (DoS) attack:** The hacker uses bots (zombies) for flooding a system with a large number of packets to render the available resources unreachable. According to some vulnerability experts, an attacker can affect more users by launching a DoS attack on cloud (Sqalli et al, 2011).
- **Insider attack:** This is when a former or current associate of the service provider with privileged access and authority performs modifications in the environment (Gaithersburg, 2001). This is fatal as many attacks can be executed from inside and an intruder can easily evade detection in the absence of proper controllers (Voorsluys et al, 2010).
- **Port scanning:** This is used by the attacker to obtain information about open, closed, filtered, and unfiltered ports (Modi, 2013).
- **User to Root (U2R) attack:** Here, the intruder accesses the credentials of an authentic user and then exploits the system vulnerabilities to access root privileges. In the network, the attacker first accesses an instance and exploits its vulnerabilities to achieve root privileges of a virtual machine or host. By this attack, integrity of the network is being violated (Modi, 2013).
- **Attacks on Virtualization:** If an attacker compromises the hypervisor, the virtual machines can be easily infiltrated (Modi, 2013). Since many virtual machines use the same resources, side channel data is vulnerable due to this type of access among virtual machines (Roberts, 2013).

2.2 Intrusion Detecting Systems (IDS) s:

IDSs are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems (Rebecca and Peter, 2001). IDSs are one of widely used security technologies. An IDS alerts the

system administrators about attack when it detects signature of accident according to host or network security policy. An IDS can be installed in a host or a network according to purpose. An IDS detects attacks based on lots of rules each of which have unique signatures that describes attack patterns. So, the detection power of IDS increases when the number of rule grows. However the existence of more rules means that each incoming packet needs to be compared with more patterns. Thus large scale of rule causes system to become overloaded.

2.2.1 Types of IDS:

According to the method of the collection of intrusion data, all the intrusion detection systems can be classified into two types: host-based intrusion detection systems (HIDSs), which analyze audit data collected by an operating system about the actions performed by users and applications; and network-based intrusion detection systems (NIDSs) analyses data collected from network packets.
Log Management: log is said to be a documented record of events. So log management would be the overseeing and managing of these recorded events. Because an IDS observes the traffic from each VM and generates alert logs, it can manage Cloud Computing globally. Another important problem is log management. Cloud Computing systems are used by many people, therefore, they generate huge amount of logs. So, system administrators should decide to which log should be analyzed first (Lee et al, 2011).

2.3. Review of Related Works

IDS/IPS Technique	Characteristics / Advantages	Limitations / Challenges
Misuse detection	Identifies intrusion by matching captured patterns with preconfigured knowledge base. High detection accuracy for previously known attacks. Low computational cost.	Cannot detect new or variant of known attacks. Knowledge base for matching should be crafted carefully. High false alarm rate for unknown attacks.
Anomaly detection	Uses statistical test on collected behavior to identify intrusion. Can lower the false alarm rate for unknown attacks	Lot of time required to identify attacks. Detection accuracy is based on amount of collected behavior or features.
ANN based IDS	Classifies unstructured network packet efficiently. Multiple hidden layers in ANN increase efficiency of classification.	It requires lot of time at training phase. Large number of samples required for training effectively. Has lesser flexibility
Fuzzy Logic based IDS	Used for quantitative features. Provides better flexibility to some uncertain problems	Detection accuracy is lower than ANN.
Association rules based IDS	Used to detect known attack signature or relevant attacks in misuse detection.	It cannot be used for totally unknown attacks. It requires more number of database scans to generate rules. Used only for misuse detection
SVM based IDS	It can correctly classify intrusions, if limited sample data are given. Can handle massive number of features	It can classify only discrete features. So, preprocessing of those features is required before applying
GA based IDS	It is used to select best features for detection. Has better efficiency.	It is complex a method. Used in specific manner rather than general
Hybrid Techniques	It is an efficient approach to classify rules accurately	Computational cost is high.

3. PROPOSED SYSTEM AND IMPLEMENTATION

3.1 The Proposed System

The proposed system is an enhanced network security system that uses intrusion detection and manages log. This system will have a Cloud File Tracker (CFT) module which manages the authentication, authorization, and accounting of the users. This model would also implement hashing encryption algorithm for securing access through the browser address. The system uses a database to store and manage user information, system logs, transaction of users and system. System managers can quickly cope with the non-predictable situation in a network through the assistance of the database that periodically intercommunicates with CFT and host OS.

3.2. Methodology

The methodology used is the Object-Oriented Analysis and Design Methodology (OOADM). This method requires objects, which integrate both behaviors (processes) and states (data) modeled after real world objects that the system interacts with unlike other methodologies where processes and data are considered separately. The aim of OOADM is to find the objects, organize the objects and describe how the objects interact. OOADM techniques are an attempt to eliminate the separation of concerns between data and processes. In the attempt of merging the data and process concerns into a single object, OOADM introduce object diagrams that document a system in terms of its objects and interactions.

3.3. Implementation

The Network security System was developed using HTML, CSS, PHP and MySQL. It has two main modules; these modules describe how the system interacts to perform tasks.

- **Administrators Module:** This provides the administrator access to manage and maintain the system. The administrator creates account for the users, adds company IP address, and also monitors the system.

User Registration Specification

Figure 2. User Registration

Adding Files Specification

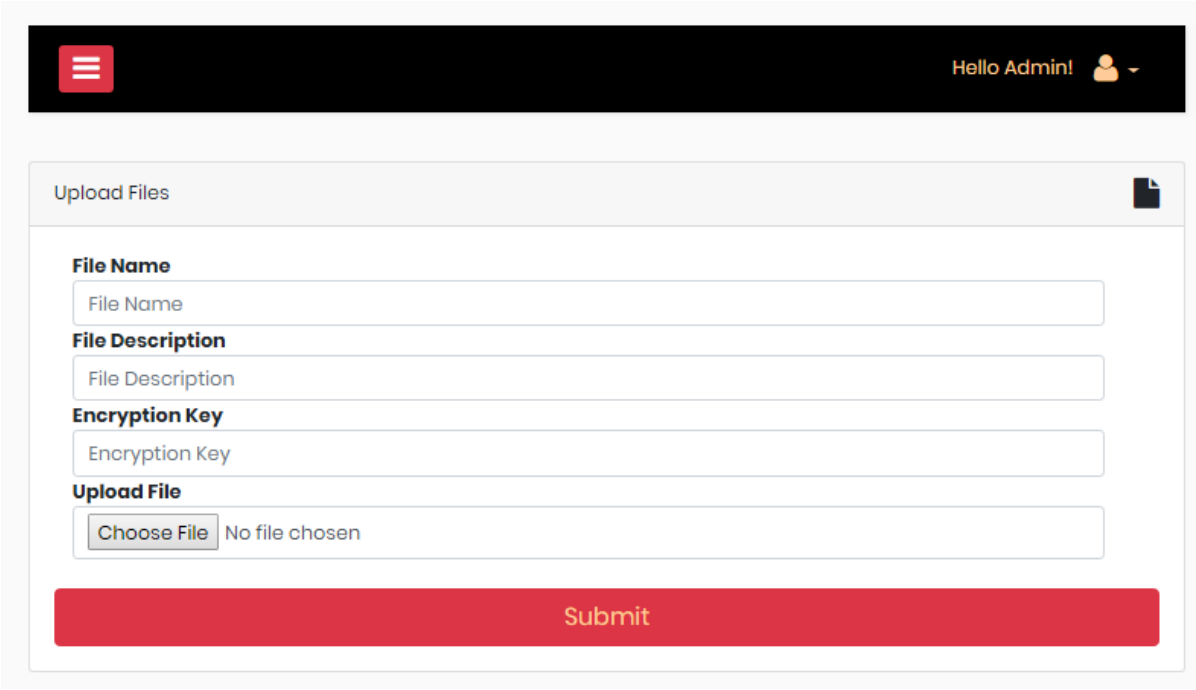

Figure 3: Add File

- **User Module:** This gives access to registered users to access the system. The system captures the users' username, password, mac Address, and IP address. This module also checks if the user is authentic or fraudsters.

User Login and Network Parameters Traffic Specification:

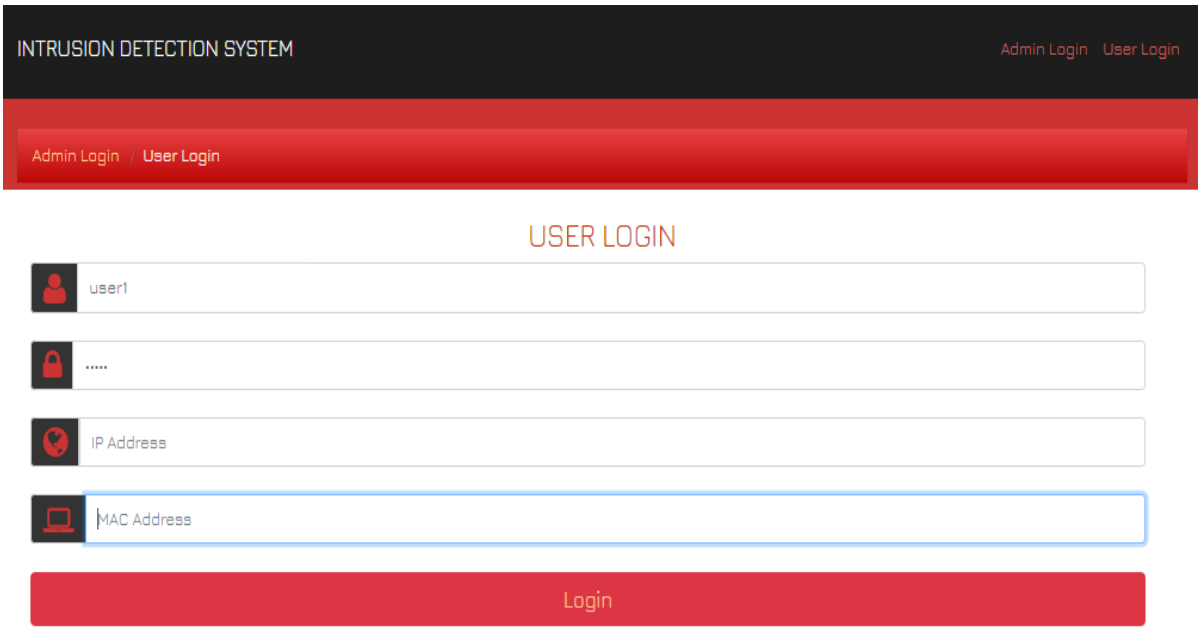

Figure 4: User Login and Network Parameters

4. RESULT AND DISCUSSION

After the development of the network security system, a test run was conducted and the system responded quite well in detecting intrusion and keeping an event log as advertised. But for the user to get the optimum use of the system some things must be in place, the hardware and software.

As the computers and networked systems increases in the world of today, the need for increase in strong network security also becomes increasingly necessary and important. The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure; one can see that the need for increase in network security is vital and important in every organization. When implementing a security plan, it is important to begin by implementing the most obvious protections first, protection of servers and routers by using passwords allowing only authorized users. Then deploy a network security system that is capable of the most advanced protections. Finally, the increase in physical infrastructure as well as its growing implication to an organization has created the necessity to physically protect the systems themselves, not only from cyber-attacks, but also from the physical attacks that can be perpetrated against them.

REFERENCES

Gaithersburg, M. D. "Invulnerability Requirements for Cryptographic Modules," National Institute of Standards and Technology (NIST), Federal Information Processing Standards 140- 2, 2001, May 25.

Lee, J. H., Park, M. W., Ecom, J. H. (2011), Multi-level Intrusion Detection and Log Management in Cloud Computing IEEE computer society, pp 552-555.

Maltais, M. (26 April 2012). "Who owns your stuff in the cloud?". Los Angeles Times. Retrieved 2012-12-14.

Martin Roesch (1999). Snort-lightweight intrusion detection for networks. Proceedings of LISA '99: 13th Systems Administration Conference Seattle, Washington, USA, November 7–12, 1999.

Mattord, V. (2008). Principles of Information Security. Course Technology. pp. 290–301. ISBN 978-1-4239-0177-8.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M. "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42-57, 2013.

Reed D., Network Model to Information Security. Retrieved: November 21, 2003. Available at: http://www.sans.org/reading_room/whitepapers/protocols/applying-osilayer-network-model-information-security_1309

Roberts II, J. C. and Al-Hamdani, W. "Who can you trust in the cloud?: a review of security issues within cloud computing," Proceedings of the 2011 Information Security Curriculum Development Conference, pp. 15-19, 2011.

Sqalli, M. H., Al-Haidari, F. and Salah, K. "EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing," Utility and cloud computing (UCC), 2011 Fourth IEEE International Conference on, pp. 49-56, 2011.

Voorsluys, W., Broberg, J. and Buyya, R. "Introduction to cloud computing," Cloud computing: Principles and paradigms, pp. 1-44, 2011.

Whitman, M. E., Herbert, J., Mattord, H. J. (2009). Principles of Information Security. Cengage Learning EMEA. ISBN 978-1-4239-0177-8. Retrieved 25 June 2010.

Zhong, H., Jun, S. and Shirochin, V. P. "An Intelligent Lightweight Intrusion Detection System with Forensic Technique," 4th IEEE Workshop on Intelligent Data Acquisition and Advanced ComputingSystems: Technology and Applications, 2007. IDAACS, 2007, pp. 647-651.