An Intrusion Detection System Application for an Organisation

P. Enyindah
Department of Computer Sciences,
University of Port Harcourt,
Choba, Nigeria.

Uzochukwu.C Onwuachu
Department of Computer Sciences,
Imo state University,
Owerri, Nigeria.

ABSTRACT
This paper is aimed at developing an Intrusion Detection System (IDS) that will guarantee the integrity of data housed in databases and connected through a network to other computers. There is need to protect clients’ and organization’s sensitive information as well as gain the benefits of Information Technology without compromising reliability of information. The objective of this software is to detect and track down details of intrusion attempt by unauthorized users such as cases of Internet Fraud. The Structured System Analysis and Development Methodology (SSADM) is adopted to developing this system as it aids effective analysis of the above problem using a series of well defined steps that builds upon each other. The development is done using technologies such as html, css, javascript for its frontend; php for its backend and the Mysql database technology for an organized data collection. The expected result will be a network based Intrusion Detection System that will help prevent unauthorized access to a network and its linked data.

Keywords
Intrusion Detection System, Internet Fraud, Unauthorized user, Information technology and Database

I. INTRODUCTION
An intrusion is an attempt by someone (“hacker” or "cracker") to break into or misuse a system. An intrusion detection system (IDS) is an active process or device that analyzes system and network activity for unauthorized entry and/or malicious activity. The way that an IDS detects anomalies can vary widely; however, the ultimate aim of any IDS is to catch perpetrators in the act before they do real damage to resources. Along with this, there is the arms race between the intruders and people who provide security to the systems in networks [14]. An IDS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyze data integrity, and more. [9] Depending on the detection methods you choose to deploy, there are several direct and incidental benefits to using an IDS. This paper IDS (Intrusion Detection System) runs on the host machines and assists the network Administrators to detect several intrusion attacks and inform to the owner of the system and also provide security by blocking the malicious users based on their IP addresses.

2. LITERATURE REVIEW
Safiqul and Syed (2011), Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches, in their work mentions several attacks on WSN and major focus is on the anomaly based intrusion detection system. Finally, they discuss on several existing approaches to explain how to identify security threats and implement the intrusion detection system [4].

Lata and Indu (2013), Study and Analysis of Network based Intrusion Detection System, Their work was on the signature based intrusion detection system methodology. They indicated that Intrusion can be possible on the header part. They employed different pattern matching algorithms are for detection intrusion. Brute force and Knuth-Morris-Pratt are two single keyword pattern matching algorithms that detect the payload part intrusion. String matching is in finding one or more occurrences of a pattern in a text (input). Snort and Sax2 are network based intrusion detection system. These systems monitor the network and capture packets in promiscuous mode, analyze these packets and gives report [6].

Mohammad et al (2012), An Implementation of Intrusion Detection System Using Genetic Algorithm, they present an Intrusion Detection System by applying genetic algorithm to efficiently detect various types of network intrusions. Parameters and evolution processes for GA were discussed in details and also implemented. Their approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity [8].

Snehal and Priyanka (2010), Wireless Intrusion Detection System, in their work said that intrusion detection system engine is the control unit of the system. Its main purpose is to manage the system, which includes proper supervision of all operations of the intrusion detection system. Its duty depends on the intrusion detection method used [5].

Suresh et al (2013), Importance of Intrusion Detection System with its Different approaches. Their work presented two types of AI system, both supervised and unsupervised [7].

Vijayarani And Maria (2015) Intrusion Detection System – A Study, their work provides a complete study about the definition of intrusion detection, history, life cycle, types of intrusion detection methods, types of attacks, different tools and techniques, research needs, challenges and applications [10].

Ahmad et al (2014) Intrusion Detection and Prevention Systems (IDPS) and Security Issues, Scanning and analyzing tools to pinpoint vulnerabilities, holes in security components, unsecured aspects of the network and deploying of IDPS technology were discussed [9].

Amrita and Brajesh (2012), An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols, their work focus on different types of attacks on IDS, it gives a description of different
attack on different protocol such as TCP, UDP, ARP and ICMP [3].

Iman et al (2011) Host-based Web Anomaly Intrusion Detection System, an Artificial Immune System Approach. They proposed the use of a novel approach inspired by the natural immune system. The capability of the proposed mechanism is evaluated by comparing the results to some well-known neural networks. The results indicate high ability of the immune inspired system in detecting suspicious activities [1].

Amrit and Manik, (2014) Analysis of Host-Based and Network-Based Intrusion Detection System, they perform log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting and active response. While Snort Network-Based Intrusion Detection System is a lightweight intrusion detection system that can log packets coming across any network and can alert the user regarding any attack. Both are efficient in their own distinct fields [2].

Santos et al (2013), Intrusion Detection System- Types and Prevention, The work aims at providing a general presentation of the techniques and types of the intrusion detection and prevention systems. Also an in-depth description of the evaluation, comparison and classification features of the IDS and the IPS. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. An IPS is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information [11].

Arul, (2011), Network Security Using Linux Intrusion Detection System, intelligent system that can detect attacks and intrusions was developed. The tool GRANT (Global Realtime Analysis of Network Traffic) being a Linux based Intrusion Detection System(IDDs), takes the advantage of the security of a Linux box and secures the other nodes in the perimeter of the network [12].

Azhagiri et al (2015), Intrusion Detection and Prevention System: Technologies and Challenges, Their work provides an overview of IDPS technologies. It explains the key functions that IDPS technologies perform and the detection methodologies that they use. Next, it highlights the most important characteristics of each of the major classes of IDPS technologies [13].

Shilpi and Roopal (2012), Intrusion Detection System Using Wireshark, IDS is to detect intrusion in network to provide safe and intrusion free network by using Wireshark. Wireshark is used to analyze network data and then that data is classified into normal data and abnormal data [15].

3. MATERIALS AND METHODS
The detailed requirements are captured in Case diagram of the proposed system as shown in figure 1.

Client's registration: This is done by both the client and the admin. The client enters his/her necessary details and the admin registers these details.

Store client's record: This is done by the admin who stores all the necessary information provided by the customer in the database to aid easy retrieval when needed.

Admin registration: This is done by the admin. New administrators can be registered to have access to the application.

Fig. 1: Case Diagram of the Developed System

Store admin record: This is done by the admin who stores the details of new administrators in the database for easy retrieval.

Client's inbox: This is owned by the client. It contains alert notifications to clients to aid intrusion detection.

Fund transfer: This is done by the admin and the client. The client enters his account details first for verification before a fund transfer is made. These details are however verified by the admin. Other verification follows during the proper fund transfer.

Feedback: Both the client and admin send a feedback. The client can lay a complaint which could be an expression of suspected intrusion on his account and the admin can as well reply to the feedback.

Generate Report: Report can be generated by just the admin.

3.1 Algorithms of Developed System
The algorithm implemented for the design of the Intrusion Detection System comes in two phases; Client Login and Admin Login.

Algorithms of Client Login

Step 1: Before a client would have access to the application, then he would get registered first. The registration details to be provided include: first name, last name, phone number, address, email, username, password, security question, answer and sex.

Step 2: Proper validation of the details is performed.

Step 3: If validation is successful is successful, the details of the client is stored in the database and he is notified through a message on the application
interface that his registration was successful. He then moves to step 4, else he goes back to step 1.

Step 4: The registered client goes to the login page through the “login link” provided. Here, he provides his username and password.

Step 5: The details are validated i.e checked for correctness. If validation is successful, he then Moves to step 6.

Step 6: The client is redirected to his page where he could check his inbox for alert notifications, transfer fund, manage account and contact the administrator in case of suspected intrusion. However, if validation fails, he is denied login. As such, he either repeats step 5 or goes back to step 1.

Algorithms of Admin Login

Step 1: An intended admin is registered by the System Administrator directly from the database. The registration details to be provided include: first name, last name, address, email, username, password, department and sex.

Step 2: Proper validation of the details is performed.

Step 3: If validation is successful is successful, the details of the admin is stored in the database and he is notified through a message on the application interface that his registration was successful. He then moves to step 4, else he goes back to step 1.

Step 4: The admin now goes to the login page provided. Here, he provides his username, and password.

Step 5: The details are validated i.e they are checked for correctness. If validation is successful, he then Moves to step 6.

Step 6: The admin is redirected to his page where he can view all received messages from clients, manage his account, create admin and contact clients, view all alert notifications on fund transfer made by clients as well as generate report. However, if validation fails, he is denied login. As such, he either repeats step 5 or goes back to step 1.

4. EXPERIMENT AND RESULT

The welcome page as shown in figure 2 is also referred to as the Index Page. This is an authentication page for registered users. However, the system validates the data of this field. If validation is successful, the user is redirected to his page, else he is returned on the same home page.

The client’s registration page as shown in figure 3 provides those necessary details /information that a new individual would have to supply in order to get registered. These details comprise first name, last name, email, address, username, password, security question, answer and sex after which the register button will be clicked to get the new client registered and as such a message displays “your registration was successful”.

Fig. 3: Client’s Registration

The page shown in figure 4 allows a client to view all alert notifications from every fund transfer made and this helps to aid detecting intrusion. If transactions are not monitored, then intrusion cannot be detected. Thus, this page displays the receiver’s account name, receiver’s account number, receiver’s bank, amount transferred, sender’s IP address, the country, city and region the client was when the transfer was made. If the client logs into his account and sees information of this nature when such transfer was not by him, he then sees it as an intrusion by someone into his account. As such, he would have to report to the administrator directly from the application to avoid further damage and track down the intruder.

4. EXPERIMENT AND RESULT

The welcome page as shown in figure 2 is also referred to as the Index Page. This is an authentication page for registered users. However, the system validates the data of this field. If validation is successful, the user is redirected to his page, else he is returned on the same home page.

The client’s registration page as shown in figure 3 provides those necessary details /information that a new individual would have to supply in order to get registered. These details comprise first name, last name, email, address, username, password, security question, answer and sex after which the register button will be clicked to get the new client registered and as such a message displays “your registration was successful”.

Fig. 3: Client’s Registration

The page shown in figure 4 allows a client to view all alert notifications from every fund transfer made and this helps to aid detecting intrusion. If transactions are not monitored, then intrusion cannot be detected. Thus, this page displays the receiver’s account name, receiver’s account number, receiver’s bank, amount transferred, sender’s IP address, the country, city and region the client was when the transfer was made. If the client logs into his account and sees information of this nature when such transfer was not by him, he then sees it as an intrusion by someone into his account. As such, he would have to report to the administrator directly from the application to avoid further damage and track down the intruder.

Fig. 4: Inbox showing alert messages for all transfer made some which were detected intrusion.
The page shown in figure 8 enables a client to manage his/her own account. In this case, he can change his password if he wishes to. The details to be provided include email of client, new password, confirm password, security question and answer. After these details are entered, the “Update” button is clicked so as to effect the change on the password.

Figure 9 is reserved to enable a client contact the administrator whenever an intrusion into his account is detected as well as provide an instant feedback to the admin. This feedback could be an expression of satisfaction/dissatisfaction of transaction made. As soon as the message is sent, a notification appears on the interface informing the client that his message was successfully sent.

The report section is one of the major functionalities incorporated in the admin’s page. This functionality enables the admin to view all fund transfer made as well as generate the report in soft or hardcopy by clicking on the “Print Report” button. See figure 10 below.
5. RESULT DISCUSSION

The welcome page as shown in figure 2 is also referred to as the Index Page. This is an authentication page for registered users. However, the system validates the data of this field. If validation is successful, the user is redirected to his page, else he is returned on the same home page.

The client’s registration page as shown in figure 3 provides those necessary details information that a new individual would have to supply in order to get registered. These details comprise first name, last name, email, address, username, password, security question, answer and sex after which the register button will be clicked to get the new client registered and as such a message displays “your registration was successful”.

The page shown in figure 4 allows a client to view all alert notifications from every fund transfer made and this helps to aid detecting intrusion. If transactions are not monitored, then intrusion cannot be detected. Thus, this page displays the receiver’s account name, receiver’s account number, receiver’s bank, amount transferred, sender’s IP address, the country, city and region the client was when the transfer was made. If the client logs into his account and sees information of this nature when such transfer was not by him, he then sees it as an intrusion by someone into his account. As such, he would have to report to the administrator directly from the application to avoid further damage and track down the intruder.

This page enables a client to transfer fund to another’s account. In this case, the client’s account name, account number and bank need to be verified first as seen in figure 5. If however the verification is successful, the client can then go further to do a fund transfer as seen in figure 6. However, every online fund transfer requires details such as the receiver’s account name, number and bank, card type (just visa and master card is required here), card number (16 digit number), card security code and amount to be transferred. After successful transfer, a transaction receipt is generated for the client as evidence of transfer made.

The page shown in figure 8 enables a client to manage his/her own account. In this case, he can change his password if he wishes to. The details to be provided include email of client, new password, confirm password, security question and answer. After these details are entered, the “Update” button is clicked so as to effect the change on the password.

Figure 9 is reserved to enable a client contact the administrator whenever an intrusion into his account is detected as well as provide an instant feedback to the admin. This feedback could be an expression of satisfaction/dissatisfaction of transaction made. As soon as the message is sent, a notification appears on the interface informing the client that his message was successfully sent.

The report section is one of the major functionalities incorporated in the admin’s page. Figure 10 functionality enables the admin to view all fund transfer made as well as generate the report in soft or hardcopy by clicking on the “Print Report” button.

6. CONCLUSION

The results obtained from this system helps efficiently in tracking down and preventing crime. From the sample output shown, this system can aid investigation and crime control. A verdict can be arrived at in good time if this information is readily available. This system should be implemented in ongoing software applications and already developed systems as it will go a long way in helping to combat crime most especially Internet fraud.

The IDS is designed to provide the basic detection techniques so as to secure the systems present in the networks that are directly or indirectly connected to the Internet. With this, at the end of the day it is up to the Network Administrator to make sure that his network is out of danger. This software does not completely shield network from Intruders, but it helps the Network Administrator to track down bad guys on the Internet whose very purpose is to bring your network to a breach point and make it vulnerable to attacks.

Thus, the expected result will help prevent unauthorized access to a network and its linked data through consistent notification/feedback to clients and organizations as activities are being carried out on the network.

7. REFERENCES


International Journal of Computer Science and Network Security, VOL.14 No.11,


