An Empirical Evaluation of the Effectiveness of the Computer-Based Network Security and Firewall in Banking Systems

[1]Sarumi J.A. (PhD), Longe, O.B. & Adelodun, F.O.
[1]Department of Computer Technology, Lagos State Polytechnic, Ikorodu, Lagos State, Nigeria
[2]Faculty of Computational Sciences & Informatics, Academic city University College, Accra, Ghana
[3]Department of Computer Studies, The Polytechnic, Ibadan, Nigeria
E-mails: [1]sarumi.j@mylaspotech.edu.ng; [2]Olumide.longe@acity.edu.gh; [3]adelodunfelicia@gmail.com

ABSTRACT

As more banking operations are migrated into the digital platform, customers have continued to enjoy better seamless banking services. In consonance with this, concerns have also continued to rise about the effectiveness of the strategies adopted by banks to mitigate different forms of attackers targeted at operational platforms by unscrupulous elements. Using a case study, this paper evaluates the effectiveness of the Computer-Based Network Security and Firewall In banking Systems. This study employed the use of online questionnaires as a means of data collection. Our study adopted the survey method to access the subject matter. Findings from the research showed that Nigerian banks rarely experience malicious attacks of any form on their systems and equally identified network security strategies adopted by Nigerian Banks. An application was developed using C# to further contribute towards the security of banking systems

Keywords: Banks, Systems, Security, network, cybercrime, Fraud, Cyber Criminals

1. BACKGROUND OF THE STUDY

The interconnection of computer with other related office equipment are finding increasing application in almost all field of human endeavor; most especially the financial sector. More and more banks are introducing the use of computer networks in their establishment.
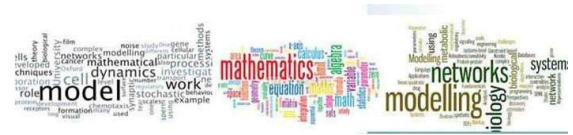
These provide for easy access to the information and services available in the organization. As a result of the high value of information, organizations now classify their data as well as putting a lot of effort to safeguard it. Networking is the vehicle for sharing information where as network security is a way to protect the information, information sharing cannot be constrained by physical or geographical location and today's information has been made accessible to all by means of global network.

For an organization to become parts of this global network, it first need to have his own Local area network (LAN), which is then connected to the internet by means of a Wide area network (WAN). The objective of network security is to control access to corporate and government data residing on network services or transmitted over the LAN or WAN.

Access Bank plc, commonly known as **Access Bank**, is a Nigerian multinational commercial bank, owned by Access Bank Group. It is licensed by the Central Bank of Nigeria, the national banking regulator. Originally a corporate bank, the organization acquired personal and business banking platforms from Nigeria's International Commercial bank in 2012.

Access Bank is presently one of the five largest banks in Nigeria in terms of assets, loans, deposits and branch network. The merger of Access Bank and Diamond Bank on 1 April 2019 has made Access Bank the largest bank in Africa. In conclusion of its merger with Diamond Bank, Access Bank Plc, unveiled its new logo, signaling the commencement of a new enlarged banking entity.

1.1 Analysis of Case Study

The introduction of information and communication technology in Banking sector is a trust-based institution, that requires an absolute trust from her customers, upon this the banking sector should take security issues as a special concern to continually earn the trust of their customers, The need to tighten-up security and proper management channels that could give opportunities for fraud and malicious attacks such as: breach of privacy of customer data, distributed denial of service attacks, and technological letdowns created on electronic banking platforms becomes expedient. Insecurity has been a major concern in the world's most prominent sector (finance), bank accounts, transactions and funds transfer are tampered with as a result of this insecurity, which is constantly being faced by operators of the banking sector.

These experiences have become totally unfavorable, which have made the total adoption of technologies in the banking sector difficult. The insecurity issue has been caused by the ripple effects malicious attacks and threats like State-sponsored espionage, Distributed denial of service (DDoS) attacks, password management, insider threat, privacy laws and viruses among others. Thus, this research is aimed at evaluating the computer and network security strategies employed by Nigerian banks.

The following objectives that were used to achieve the aim were: the determination and identification of the security strategies which are being implemented by banks in Nigeria, ascertaining the impact of various integrated banking system on the total security of the banking sector, to assess the security strategies employed by Nigerian banks and also evaluate its effectiveness.

1.2 Statement of the Problems

Access bank Nigeria limited (Bariga) has a large volume of information, which it has to handle efficiently in other to evolve efficient corporate management and improved customer services. The information needed to carry out operation geared toward customer satisfaction must be highly secured and transmitted properly too. Since the banks uses computer network in their activities, there are bound to be threats to security which hinders work progress in the organization, once the organization launches its presence in the internet.

Most banks lack awareness on how a network can be implemented, secured and maintained.
1. Threats to network security are sometimes difficult to track and it won't be easy to refuse the request of the attackers.
2. Without refusing legitimate request for services. This attack comes from any connection that the bank has with the outside world, which included dial up moderns, and internet connection. So in order to adequately address security all possible avenues of entry must be identified and evaluated, also the security of every point must be consistent with stated policy on acceptable risk levels.

1.3 Objective Of The Study

Networking is the backbone of accessing vital information. The world has becomes a global village, sharing everything through networking. Networks requires a high level of security, which involves the technical and administrative safeguards required to protect a computer based system (hardware, personnel data) against the major hazards to which most computer system are exposed and to control accessed to information.
1. This work is aimed at defining/providing a security system that will keep unauthorized users from the protected areas of the network.
2. This system will also prohibit potentially vulnerability services from entering or leaving the network.
3. To develop a standalone application that will exhibit the security features of a banking system
4. The system will also provide a location for monitoring security related events and adults as well as the overall security management of the network.

1.4 Scope of the Study

This study presents an overview of security system network and firewalls its highlights are on firewalls. Risks threats and vulnerability of network. It also concentrates on design of security system and network types an its computer application.

5ignificance Of The Study

i. Security and fire walls are useful in banking sectors and in their services
ii. It is useful to the banks in other sectors who would wish to use network security and firewall in their banks.
iii. It shows need for security in banking sectors.
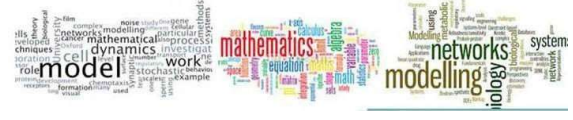
2. RESEARCH METHODOLOGY

The population of study is limited to computer security experts and information technology department staff in Access bank, Bariga. purpose of this study was to evaluate how effective computer and network strategies put in place by Nigerian bank, Access bank, Bariga branch.

This study strives to provide answers to the under-listed research questions:
i.   What banks do the respondents work for?
ii.   What are the years of experience of the respondents?
iii.   What Computer security strategies are implemented?
iv.   Why is a particular anti-virus preferred to other antivirus software?
v.   How often has the bank suffered malicious attacks?
vi.   vi. Why is a particular integrated banking system (Core Banking System) preferred to other CBS software?
vii.   How effective are the computer strategies implemented?

2.1 Observation And Interview Carried Out.
The main method of research concerning this project is by observation and interview with a professional system application developer who has experience in developing Windows application using C#. We had five minutes chat on the best programming language to use, the model and how wireless networks can be secured effectively. I also did a documentation from my observation on how wireless networks or prone to attack without effective security measure.

2.2 Sources Of Data
The data that were collected in this research were from the primary sources. Observations were made while carrying out practical on the operations of wireless networks like WIFI on mobile devices without security, I did research on the most suitable programming language to use . Other sources of data were of the secondary source, which includes gathering information from journals and magazines, materials from internet, Microsoft Encarta premium, seminars, lectures and personal researches.

3. SYSTEM DESIGN AND DEPLOYMENT

3.1 Problems Associated With The Current System
The primary problem common in Wireless network without firewall is lack of data protection, Privacy Bridge, malicious attacks on proxy, loss of files and incessant accesses on devices without the awareness or permission of network owner.

3.2 The New System Design
In the process of evaluating the solution and the specifications of a detailed computer based solution, there is need for the system design. In designing the new system, the software and hardware aspects were taken into considerations in order to produce a workable program that will allow effective, efficient and secure use of wireless network.

a) **PROGRAMMING LANGUAGE:** This application is developed C#. This sophisticated programming language allows the programmer to effectively carry out effective security features on a wireless network.

b) **USER INTERFACE DESIGN:** It is a system that permits the interaction between human beings and the computer. The project has a user interface design because of the level of interaction where the input and output of the system will be carried out.

c) **PROCEDURAL DESIGN:** This involves the design of an efficient algorithm that will satisfy the functional description of the various sub systems.

d) **PROGRAM MODULE SPECIFICATIONS WITH FIREWALL:** These are the program module:
   i. Home page
   ii. Rectification of connected devices
   iii. Management of devices base on access point
   iv. Action (Decline / Approve base on threat level)

3.3 Wireless Router Network and Secure Wireless LAN

A wireless router connects directly to a modem by a cable. This allows it to receive information from — and transmit information to — the internet. The router then creates and communicates with your home Wi-Fi network using built-in antennas. As a result, all of the devices on your home network have internet access.

Figure 1: Wireless Routing
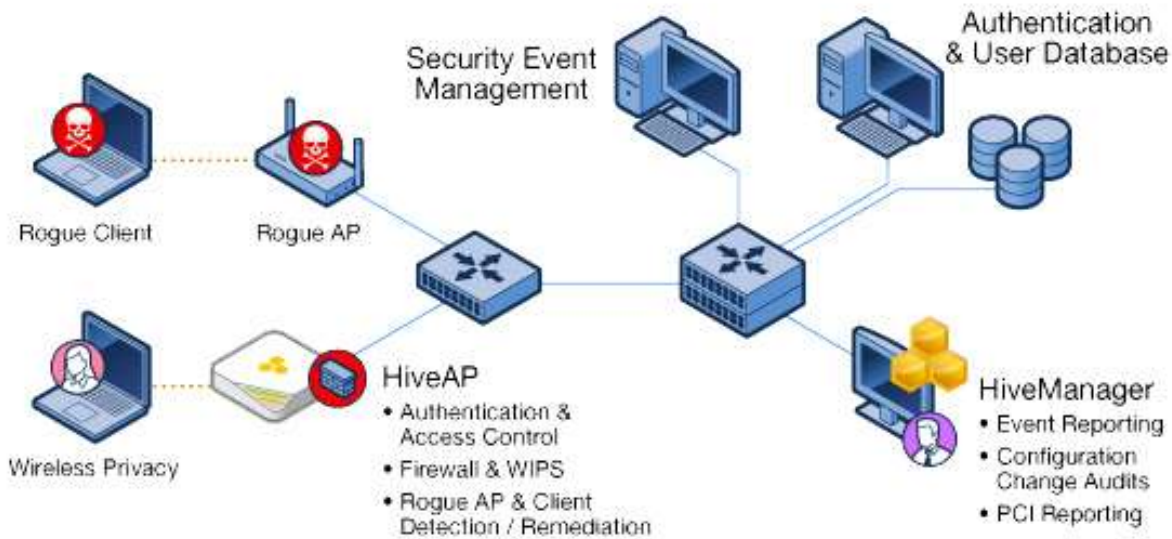Source: www.wirelessnetwork.com

Figure 2: Secure wireless LAN

Requirement Specifications: System requirements are a description of the needs, and devices a user needs for an information system. Here, unique requirements of a system are identified as user requirement. These are the installed program to carry out wireless network security system.

Choice Of Programming Language; This project is implemented with the programming languages.
C#:C# is a multi-paradigm programming language encompassing strong typing, imperative, declarative, functional, generic, object-oriented, and component-oriented programming disciplines.

Reason For Choosing C#; The system application program under development is a Microsoft windows application that assesses WIFI connection and following that C# is the generic programming language best suited for Windows app.

System Proposal: This emphasizes on the purpose of the newly designed system so as to facilitate the operations of Wireless network security. This system proposal here has come to scrutinize the old system, improve it and propose a new one which will advance the security results wireless network.

The Design Objectives: The purpose of this project is to develop security system for wireless networks to avoid hackers or any form of malicious attacks using Firewall in Access bank, Bariga branch.

4. SYSTEM DESIGN AND IMPLEMENTATION

4.1 Scope Of The Design
The scope in the design of the new system has been limited to the activities of Wireless security network with special interest on Firewalls security which is implemented on Access bank, Bariga computer application. Some of the considerable factors include.

- WIFI connection with devices.
- Security measures in it.

4.1.1   System Design
System design is a logical and creative process consisting of an integrated collection of tools and specifications of input, output etc of the system. The purpose is usually to propose a specification which will enable the complete and accurate implementation of this new system. The result of such an analysis will give rise to proper documentation of events into a document or a set of document which will enable the programmer or software engineer to start work

4.2 Input/ Output Specification and Design
The input to the new system consist of the various wireless network connection, using banking firewalls as the case study, different device types the samples are labeled according to the types of the input and also verify to determine its validity.

4.3 System Requirement to carry out WIFI security
The requirement of the new system is divided into two
1. Hardware
2. Software

Hardware
1. Pentium 111 processor
2. Speed 1.59GHZ
3. Main memory
4. Hard disk capacity 20Gb
5. Monitor 14 inch VGA
6. Ups (uninterrupted power supply)
7. Serial port two
8. Standard or enhanced keyboard

Software Requirement

Software in computer is divided into system and application software. The system software are built programs that come with the system or provided by the computer manufacturers while the application program or software are these programs that are designed to solve a particular problem.

The software requirement for the proposed system is;
1.   Minimum of Window XP operating system
2.   C Sharp programming language.

4.4 System Implementation

This is the actual process of bringing the proposed system to lift and place it in the organization. System implementation also includes creating a new system and getting it into working order. For this to be achieved it must be done in a procedure involving how to start and stop the system, entering of information and data must be documented. Although some users already have a good idea of the system while others need to be taught about it in order to be conversant with it. Here, the entire program is tested using different data and system platform. During this phase, the developer documents clearly the user trimly and instructions on the changes the new system will introduce in the area of information management and decision making.

4.4.1 Program Design

The program is designed to take care of wireless network security, respective task that constitutes WIFI connections and its implementation. The program design is based on the input and output specification to facilitate easy coding, testing, debugging and it is in module.

4.4.2 Program Testing and Debugging

C# programming language has distinct modes for developing an wireless network application. Before the program is implemented, the user must test and run it and if bug are found in the program, the developer debug the program so that the program can run without bugs when the program is free of bugs it can then be implemented fully.

4.4.3 Program Documentation

This is an important part of system development it uses the techniques and tools of system analysis and design to record and communicates the activities and result of each stay of information system development.

The hardware has all features required to best utilize the software. The software can handle the data processing assignment easily without major modification, and the language it is written in a programming language that is commonly used by wireless network application developers and user.

4.4.4   System Evaluation And Maintenance

Maintenance of the system means keeping the system running without a problem that may cause the system to breakdown. The steps outlined below can help prevent the system:

1. No usage of outside source floppy disk, flash drives or CD-Rom which may contain program that can rearrange files in the system.
2. No external bodies should be allowed to access the system
3. Anti-virus package most be installed and updated annually.
4. The system should be out of reach to unauthorized users in the organization
5. Faulty material should be changed immediately.

4.5 Training of Staff / Users

The staff / Users of the new system will be given adequate training, it involves prove decision on how well the system work, handbooks are needed for this purpose to provide detailed description on how the job is done. On rare occasions depending on the complexity of the system and the level of skill currently available courses should be organized periodically to update the staff/user knowledge. Also job aid are needed to assist staff /user to carryout instruction while performing the job. Effort should be made to work on the psychology of staff/user in order to disabuse any wrong motion or mindset they have about the new system.

4.6 Change over Procedure

This is the implementation process which the changes are made from the existing system to the newly designed one. There are three basic methods

a. Pilot Change Over: This involves changing part of the system using parable or indirect change over procedure. This procedure is a trial system implementation in a subset of the overall operation as an office geographical area.

b. Direct Change Over: This is termed immediate or crash change over using this method, the old system is discontinued and the new system is put into operation at once. For a large organization. This system is risky should there be a system failure. This approach is feasible only the timing problem becomes greater as the scale of operation increase with regard to me new system an individual can easily adapt. This system without much course to regret

c. Parallel Change Over: Is a change over procedure where the old system is run in parallel with the new system and comparison made for a whole. One merit is that, there is room for proper evaluation of the new system as to ascertain errors in any of the process. This method has been formed to be operational effective despite the fact that procedure is not cost-effective.

4.7 Documentation

Documentation is very important since it is a method of recording and communicating the activities of the system development and the outcomes of each stage in the entire process. Documentation of any system will minimize during the problem that may be encountered during modification or maintenance of the system. Documentation serves the following purpose.

i.   Eliminates duplicates and reducing of effort in the system development process
ii.   It minimizes ambiguity in the procedures
iii.   It prevents loss of key information vital to proper implementation of the system.
iv.   It provides adequate instruction for proper use of the system.

The complexity of the system documentation will normally depend on the extent of the system being developed. For instance a system being developed for a temporary use would not required a detailed documentation as the system being developed for permanent use.   Nevertheless system documentation is divided into two parts system manual and user manual.

5. PROGRAM SCREEESHOT:

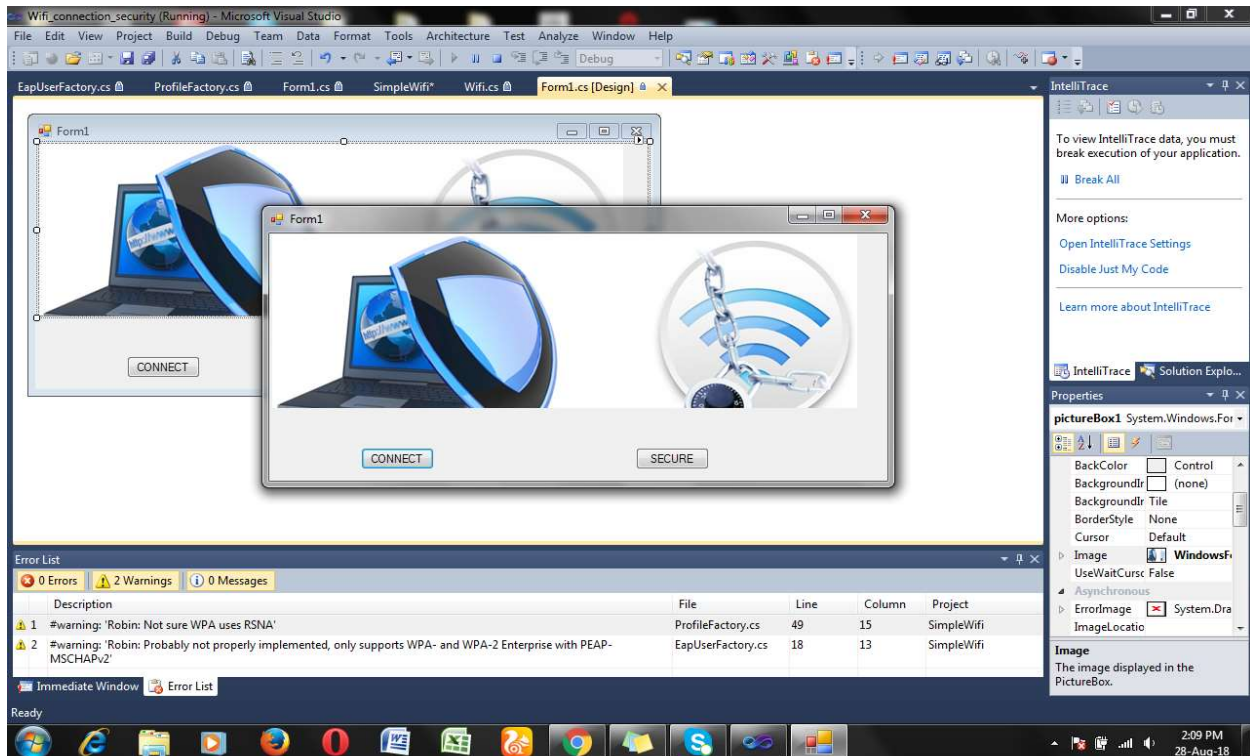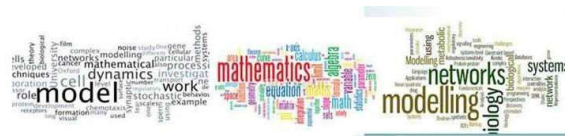Below is a screenshot of the developed artifact

Fig 3: Screenshot Of The Developed Artifact

6. CONCLUDING REMARKS

It has been identified that financial institutions are one of the major users of Information Technology hence the need to evaluate effective use of the computer security strategies. This study aimed at evaluating the effectiveness of computer and network security strategies employed in Access Bank, Bariga, Lagos state in Nigeria. This study was led by the following objectives; to determine and assess the security strategies that are put in place by Nigerian banks, to suggest solutions that would improve the effectiveness of the evaluated security strategies, to identify the effect of the various security strategies on the integrated banking system. This study employed the use of online questionnaires as a means of data collection. The study majorly focused on computer security strategies employed by the banks, and how effective the implemented security strategies have been. The strategies include passwords, antivirus, firewalls, encryption, intrusion detection systems and intrusion prevention systems, and it was mentioned that the integrated banking systems used by Nigerian banks has a certain security level thereby aiding the computer systems security in general, the study also revealed that Nigerian banks rarely experience malicious attacks of any form on their systems. The study findings revealed that Nigerian banks are implementing at least five computer security strategies.

This research evaluated the effectiveness of computer and network security strategies being used by Access bank, Bariga, Lagos state in Nigeria. And the following conclusions were drawn, from the results presented earlier. First, computer and network security strategies implemented in Nigerian banks are; passwords, encryption, firewalls, intrusion detection system and intrusion prevention system and about half of the respondents were not sure if they use intrusion detection and prevention system. Secondly, from our research the evaluation, proved that almost all Nigerian banks are fully and effectively implementing the computer and network security strategies. However, only about 15.33% of the respondents from Nigerian banks experience malicious attacks of any form in the bank's system and about 84.66% asserts that they never or rarely experience malicious attacks of any form. Finally, from our presented results, we then conclude that Nigerian banks are using effective computer and network strategies after, implementing almost all security strategies and they rarely experience malicious attacks of any form.

7. RECOMMENDATION

This research covers wide areas of use which this project can be adopted on several areas like:
i.   Further research purposes on Networking or Security
ii.   Electronics Engineering sector for developing electronic sensors and security
iii.   Schools research centers can as well use it, it is recommended for future works.
iv.   It is recommended for further development for security use on WIFI connection which can be commercialized,
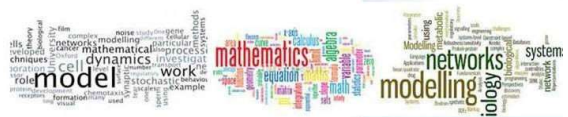
REFERENCES

1. Someto .O (2011). Data Security and Networking, 24thEdition McGrawHill, USA.
2. Abdul, P. J. (2015): Computers and Information Processing: Concepts and Applications. (14th ed.). New York, West Publishing Company.
3. Franklyn .F. (2005). Conceptual Framework: Gathering network security information. 7th ., Chicago, Crakfund.
4. Caleb .K (2015). Computerized security check systems, Boston,PWS Publishing, 4th edition, pp 53.
5. Clifford, L. (2014). Introduction to Wireless Security Network 1995 to 2004, The building block for every security system 28, pp. 93-103.
6. Locke, J. (2014):"Basics of Knowledge Engineering", Kindred Communications Troubleshooter Team, Microsoft Support Technology, December 2014
7. Kayacan, E., Ulutas, B. and Kaynak, O. (2010), Basics of computer networking, Grey system theory-based models in time series prediction, journal homepage: www.elsevier.com/locate/eswa.