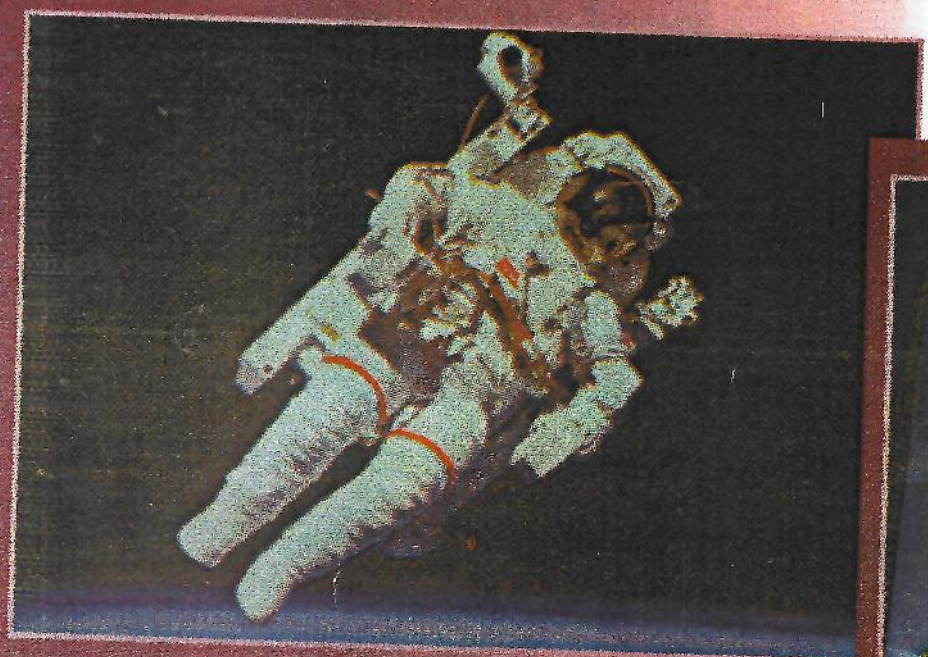
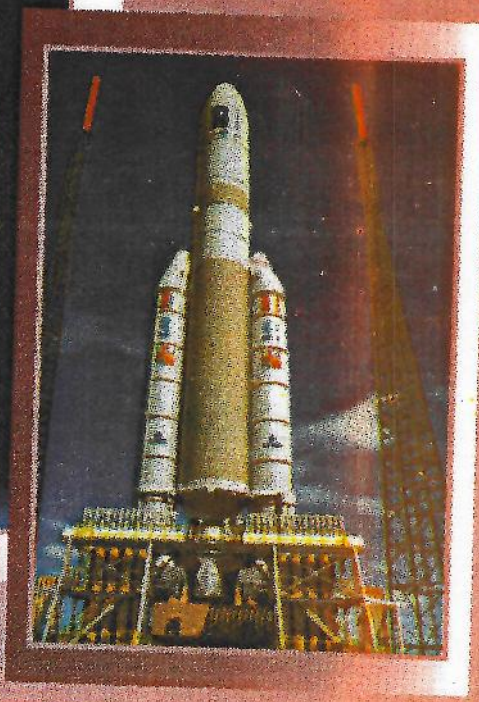
SCHOOL OF SCIENCE AND SCIENCE EDUCATION (S.S.S.E.)

FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

4th ANNUAL NATIONAL Conference





THEME:

THE ROLE OF SCIENCE, TECHNOLOGY AND MATHEMATICS IN THE ATTAINMENT OF MILLENNIUM DEVELOPMENT GOALS

Date: 4th - 6th November, 2010

Book of Readings

TABLE OF CONTENTS

OPNET IT Guru Academic Edition to Enhance Networking Education in Nigerian Universities.

S. Zubair[1]*, S. Ahmad[2#], H. T. AbdulAzeez[2$], B. A. Salihu[1&]
[1]Department of Communication Engineering Federal university of Technology Minna
[2]Department of Cyber Security Federal university of Technology Minna
*zubairman@futminna.edu.ng, #suleahmad@yahoo.com, $athassan@gmail.com,
&salbala@futminna.edu.ng

Abstract

In this paper, we present our approach on how OPNET can be easily integrated into the curricula of networking to reinforce networking theory taught in our universities. We described our teaching objectives and discussed why we choose it over other major simulation software packets. We then proposed an OPNET simulation networking laboratory that complements classroom lectures by presenting the representative projects of the OPNET simulation labs that emphasize the understanding of the dynamics of network design and contain some extension or development of the topic beyond the lecture/reading.

Key Words; OPNET, simulation, modeling, networking, active learning, hands-on experiment.

Corresponding Author: S. Zubair

Introduction

Networking education is a core area of ICT that is imperative to the attainment of Millennium Development Goals (MDGs) if properly administered. In the contemporary world, before any meaningful development can be achieved, it has to be timely measured with respect to similar developments around the globe. Hence, if a country fails to invest in establishing a solid knowledge base in networking, it is either planning to waste more fund in importing this imperative developmental recourse or it has willingly chosen to be left behind in the fast developing world. Also, as networking systems have become more complex and expensive, hands-on experiments based on networking simulation have become essential for teaching the key computer networking topics to students and professionals.

This software enhances the proper integration of the Engineering of networking into the programs of conventional, virtual and open universities. Before now, Engineering programs that need active laboratory sessions are usually either not offered or not properly administered in virtual universities. The advent of this software makes this area more accessible to a wide range of people in the country hence promoting development at large. The simulation approach is the most cost effective and highly useful because it provides a virtual environment for an assortment of desirable features such as modeling a network based on specific criteria and analyzing its performance under different scenarios with no cost.

OPNET IT Guru

OPNET IT Guru Academic Edition provides a virtual environment for modeling, analyzing, and predicting the performance of IT infrastructures, including applications, servers, and networking technologies. Based on OPNET's award-winning IT Guru product, Academic Edition is designed to complement specific lab exercises that teach fundamental networking concepts. OPNET software is used by over 500 universities (Larry & Bruce, 2003).

Integrating IT GURU

IT Guru's role in the classroom extends beyond merely learning networking technologies. Learning IT Guru is itself a worthwhile classroom objective because IT Guru is an industrial strength software with real world applications and career paths. IT

Guru's educational potential will typically be that of teaching networking technologies. The question then is how best to use it to teach networking technologies. It has numerous modules and several distinct methods of creating topologies.

The IEEE/ACM Computing Curriculum 2001 (Computing Curriculum, 2001) strongly recommends integrating hands-on experimentation and analysis into networking courses as they reinforce student understanding of concepts and their applications to real-world problems. It also has been stated that laboratory components are absolutely essential for a networking curriculum and deep understanding of networking requires laboratory facilities that allow one to build, observe, experiment, and measure (Comer, 2004).

Many different approaches have been taken in developing "hands-on" laboratory-based networking courses. While some laboratory courses focus on network management and configuration (Fitzhugh, 2002), other laboratory environments focus on one layer of networking protocols, such as implementation of transport level protocols (Richards, 2001) and link-layer network traffic analysis (Jipping, Bugaj, Mihalkova, & Porter, 2003). A few large networking education programs (Mayo & Kearns, 1999; Steenkiste, 2003) provide dedicated hardware in which students can experiment with a number of real networks and develop network functionality at the kernel level. However, such environments require extensive resources to setup and manage, and the high cost of providing dedicated networks makes it financially unworkable for most programs. The Virtual Network System (Casado & Mckeown, 2005) is a teaching tool designed to allow hundreds of students working remotely to develop user space programs that function as network infrastructure components.

Most of these networking laboratory courses are introduced as a second course in computer networks. However, due to limited faculty and facility resources, most colleges and universities are only able to offer one networking course, mostly without any laboratory components. In fact, courses that expose students to actual network environments are still mostly absent in undergraduate and graduate curriculum (Kurose, Leibeherr, Ostermann, & Ott-Boisseau, 2002). There is an urgent need to integrate introductory networking courses with laboratory components.

One way to integrate laboratory components into an introductory networking course is with simulation. Network simulation allows students to examine problems with much less work and of much larger scope than are possible with experiments on real hardware. An invaluable tool in this case is the free OPNET IT Guru Academic Edition that offers the tools for modeling, design, simulation, data mining and analysis. IT Guru can simulate a wide variety of different networks which are linked to each other. The students can therefore exercise various options available to networks and visually see the impact of their actions just by sitting at their workstations. Data message flows, packet losses, control/routing message flows, link failures, bit errors, etc. can be seen by the students at visible speed. This is the most cost effective solution for universities to demonstrate the behaviors of different networks and protocols.

As such, these practical sessions can easily be integrated into the course unit without having to slate a separate laboratory class. This can be done by giving assignments based on the hands-on labs or taking time out of the normal time of the course for practical hands-on simulation demonstrations using prepared lab scenarios. Practical problems from industries could also be presented as assignments to the students to proffer solutions. By so doing we are already exposing the students to how to tackle real life situations and this makes them better professionals in the industries.

Teaching goals

Our teaching goal is to effectively integrate laboratory components into the introductory networking course without significantly increasing the workload of both instructors and students. The main objectives of our simulation laboratory experiments are:

- To reinforce the networking theory taught in classes with hands-on experiments. In our lectures, we teach networking concepts and protocols at a relatively abstract level. We hope that hands-on lab exercises lead to a deeper understanding of networking principles and concepts.
- To allow students to build, observe, experiment, and measure variety of networks including direct link networks, switched networks, wireless networks, and inter-networks.
- To balance the breadth and depth of knowledge in an introductory networking course and drive some topics down to a level of details where students understand the elegance of the engineering that make this all work.
- To provide additional learning opportunities to discover knowledge.
- To provide an open lab environment so that all the lab experiments can be completed without supervision and in relatively short time (a few hours).

To meet these objectives, the following properties are essential for the network simulator to be used for the laboratory experiments:

- Ability to simulate a wide range of networking technologies: The simulation software could be used to model the entire network, including its routers, switches, protocols, servers, and the individual applications they support. It should support a large range of communication systems from a single LAN to global satellite networks.
- Ease of use: the simulation software should be easy to install and use. Students should be able to use the software to complete the lab assignments independently without any formal training.
- Free or low cost: The software should be free or low cost. In order to provide the open lab, students should be able to download and install the software on their personal computers.
- Higher simulation performance: For each lab assignment, students are required to create network model, run simulation, analyze results, and write a report. It is very important to have a high performance simulation engine so that simulations of most lab experiments can be completed in relatively short time (less than 30 minutes).

Other properties desired but not absolutely necessary are:

- Suitability of the software for use in research: the simulation software can be used for the simulation-based networking research.
- Better industry employment opportunities for students: the software should have a large user community and should be widely used by industry. So, students who have been taught using the software should be able to immediately apply their knowledge of network simulation when first employed.

Why OPNET IT Guru

In the market there are two major options for networking and simulation software; Boson's OPNET's IT Guru and NetSim (Network Simulator). The former appears to be more widely adopted in academia while the latter seems to target the Cisco's line of networking examination and prep markets and not necessarily networking in general. IT Guru also requires a lot of supporting software and more configurations before one can get

the software ready for simulation. IT guru is comprehensive and technology neutral in its capabilities and versatility. It does not need much of setup configurations, easy to install, free and it is more user-friendly.

IT Guru enables one to create a *virtual* network consisting of relevant hardware, protocols, and application software. Virtual network is a purely software entity that can run on an individual workstation. Routers, switches, web servers – almost anything found in real networks – can be duplicated in an IT Guru virtual network. It can be scaled from just a network of two workstations to one representing tens of thousands running in a WAN.

Once a virtual network is created it can be manipulated in various ways. For instance, routers can be added or subtracted, protocols switched around or altered, web servers added or discarded – any permutation imaginable. The effects of various alterations and diverse configurations can then be usefully and quantifiably examined and analyzed. Importantly IT Guru allows one to study and gather useful statistics about a virtual network built from it. It permits not only the building of a virtual network in software but also provides tools for dynamically investigating the thus engendered network. Hence its choice for this proposal!

Representative Projects

Our simulation labs emphasize the understanding of the dynamics of network design. Students learn, through these experiments, a wide range of networking aspects including the design of simple networks before it is being practically deployed, simulation and performance evaluation techniques, and interpretation of network analysis. Furthermore, we try to ensure that labs contain some extension or development of the topic beyond the lecture/reading and provide students additional active learning opportunities to discover knowledge.

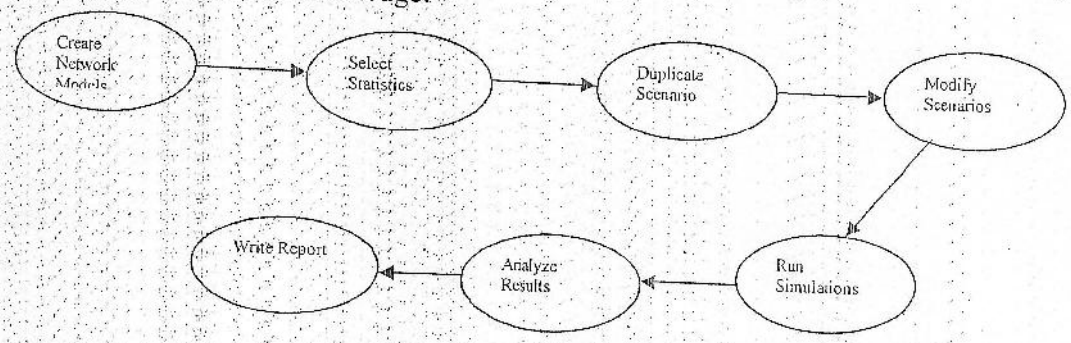


Figure 1: Workflow for Lab Experiment

Each lab experiment consists of the following seven steps: create network model, choose statistics, duplicate scenario, modify scenario, run simulations, analyze results, and write a report, as seen in Figure 1. In addition, each lab has a few questions based on the reports generated from the simulation to test the students' understanding as well as analytical and reasoning skills.

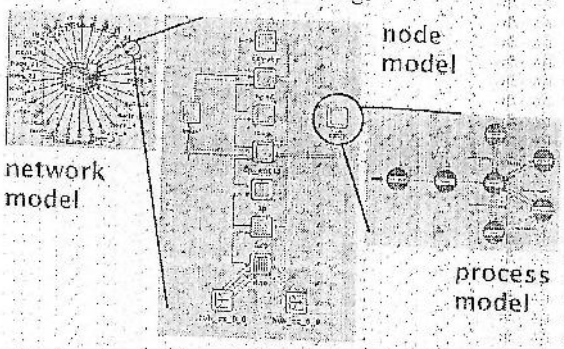


Figure 2: Network, Node and Process Models of OPNET Graphic Editors.

OPNET provides four editors to develop a representation of a system being modeled. These editors, the Network, Node, Process, and Parameter Editors, are organized in a hierarchical fashion, as seen in Figure 2. Each level of the hierarchy describes different aspects of the complete model being simulated. Models developed at one level of the hierarchy are used (or inherited) by models at the next higher level. This leads to a highly flexible simulation environment where generic models can be developed and used in many different scenarios.

We design detailed lab manuals so that all lab experiments can be completed without supervision. The following are some representative lab assignments designed around OPNET.

Laboratory 1: Ethernet Network

This lab was designed to demonstrate the operation of the Ethernet network. The simulation in this lab helps the student examine the performance of the Ethernet network under different scenarios. The student will set up an Ethernet with 40 nodes connected via a coaxial link in a bus topology. The coaxial link is operating at a data rate of 10 Mbps. They will learn how the throughput of the network is affected by the network load as well as the size of the packets as shown by the figure 3 below.

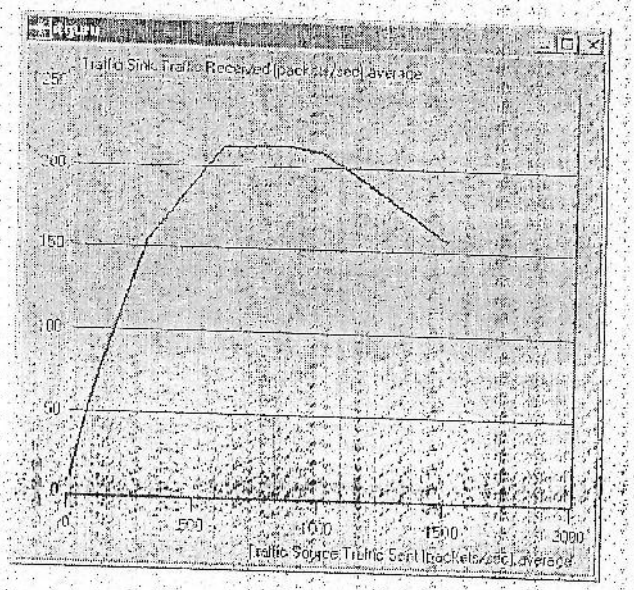


Figure 3: Result for Ethernet Lab

Laboratory 2: Switched LANs

This lab was designed to demonstrate the implementation of switched local area networks. The simulation in this lab helps the student examine the performance of different implementations of local area networks connected by switches and hubs. They will set up switched LANs using two different switching devices: hubs and switches. They will study how the throughput and collision of packets in a switched network are affected by the configuration of the network and the types of switching devices that are used.

Laboratory 3: Network Design

The objective of this lab is to demonstrate the basics of designing a network, taking into consideration the users, services, and locations of the hosts. In this lab the student will design a campus network that has six blocks: Agric, Environmental, Senate, Mechanical, Engineering and ICT. The students will utilize a LAN model that allows them to simulate multiple clients and servers in one simulation object. They will be able to define a profile that specifies the pattern of applications employed by the users of each block in the Campus. By the end of this lab, the students will be able to study how different design decisions can affect the performance of the network.

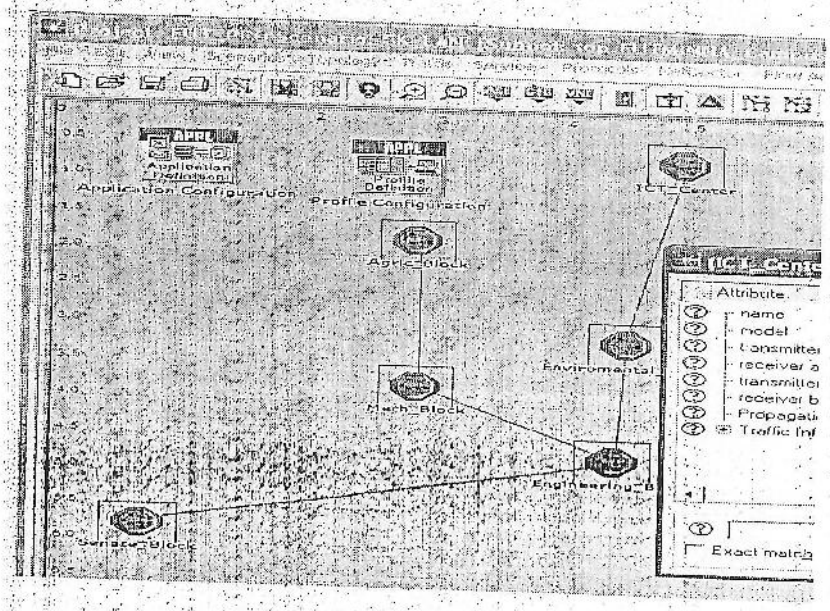


Figure 4: Network Design

Conclusions

An important complement to classroom lectures is laboratory experiments. In networking, this often implies programming, protocol design, experiments and measurement. We believe that simulation has an important role here, since it allows students to examine problems with much less work and of much larger scope than are possible with experiments on real hardware. Simulation can be easier than experimentation because simulators do not need to reproduce all the details of the real world and they can be easily instrumented. In addition, simulation of dozens or hundreds of nodes are easy on limited hardware, many more than is affordable if physical hardware was required.

In summary, students benefit from the OPNET simulation laboratory in the following three ways. First, the OPNET simulation labs reinforce the networking theory taught by regular lectures. Second, the open design of the labs encourages active learning. Third, students gain the knowledge of modeling and simulation techniques for

performance evaluation of networking systems. This active learning approach gives students experience in the subtleties of the design of a complex system, as well as prepares them for the networking industry.

References

Casado, M. & Mckeown, N. (2005). The virtual network system. *The Proceedings of the 36 SIGCSE Technical Symposium on Computer Science Education (SIGCSE'05)*, 76-80.

Computing Curriculum. (2001). *IEEE/ACM CC-2001 Task Force.* Retrieved January 6, 2006, from http://www.acm.org/sigcse/cc2001/index.html

Comer, D. (2004). *Hands-on networking with internet technologies* (2nd ed.). Prentice Hall.

Fitzhugh, S. (2002). Portable network laboratory. *32nd ASEE/IEEE Frontier in Education Conference*, Boston, MA, November 2002.

Jipping, M. J., Bugaj, A., Mihalkova, L. & Porter, D. E. (2003). Using Java to teach networking concepts with a programmable network sniffer. *Proceedings of the 34th SIGCSE Technical Symposium on Computer Science Education*, 120-124.

Kurose, J., Leibeherr, J., Ostermann, S., & Ott-Boisseau, T. (2002). Workshop report. *ACM SIGCOMM Workshop on Computer Networking: Curriculum Designs and Educational Challenges.*

Larry L. P. & Bruce S. D. (2003). Computer Networks; A Systems Approach. USA, Morgan Kaufmann, 3rd Edition (April 2003) page vii

Mayo, J. & Kearns, P. (1999). A secure unrestricted advanced systems laboratory. *The Proceedings of the 30th SIGCSE Technical Symposium on Computer Science Education (SIGCSE'99)*, 165-169.

Richards, B. (2001). Rtp: a transport layer implementation project. *Proceedings of the Sixth Annual CCSC Northeastern Conference on the Journal of Computing in Small Colleges*, 134-141.

Design of a Trapdoor for Password Access.

Ahmad, S.[2#], Zubair, S.[1] *, AbdulAzeez, H. T.[2 $], Salihu, B. A.[1&] ; L. Idris[3]; and A. Ibrahim

[1]Department of Communication Engineering Federal university of Technology Minna
[2]Department of Cyber Security Federal university of Technology Minna
[3]Department of Mathematics/Statistics Federal University Of Technology Minna
*zubairman@futminna.edu.ng, #sulcahmad@yahoo.com, $athassan@gmail.com, &salbala@futminna.edu.ng

Abstract.
Safety of data and information into computer at this computer age has constituted a serious problem because of the dubious people all around the world. This study is concerned with the development of the design of a computerized method of protecting data and communication systems against unauthorized disclosure, transfer, modification or destruction whether accidental or intentional. The trapdoor password access security system was divided into four categories which include knowledge acquisition, knowledge representation, user interface and design. The whole system is mainly based on reasoning methods that reflect human logic skills on security design. This work was able to reduce or completely eliminate system vulnerability to security threats. A new user friendly security system has been designed to ensure security of files, folders and data. The search for a more simplified means of doing this task is desirable at all time.

Key Words: Data, Trapdoor, Password.

Corresponding Author: S. Ahmad

Introduction

Design of a Trapdoor Password access is a trusted solution to securely store, access and administer shared administrative passwords. It enables information technology users to maintain a central repository of passwords, enforce standard password policies and control unauthorized user access to shared passwords. It also provides a complete record of 'who', 'what' and 'when' a password access is made in the system.

The threat of trapdoor surfaced when multiuser and networked operating systems became widely adopted. (Petersen and Turn, 1967) noted a class of active infiltration attacks that use Trapdoor (backdoor) entry points into the system to bypass security facilities and permit direct access to data. The use of the word *trapdoor* here clearly coincides with more recent definitions of a Trapdoor. However, since the advent of public key cryptography the term *trapdoor* has acquired a different meaning. More generally, such security breaches were discussed at length in security information system corporation task force report by (Anderson and Edwards, 1970).

Related Studies

Computer security is the protection of computer information from accidental or malicious modification destruction or disclosure the science and study of method of protecting data in computer and communication system against unauthorized disclosure, transfer, modification or destruction whether accidental or intentional. Password access systems have developed from a branch of computer science there is primarily concerned with security based knowledge representation, security verification, preventing unauthorized user, and the development of computers that can secure the resources of the system (Townsend, 1987).

The paper to describe black box trapdoor issues, points out that trust is relative. It describe a very clever trapdoor mechanism based upon the fact that people only review source (human-written) code, and not compiled machine code. A program called a compiler is used to create the later from the former, and the compiler is usually trusted to do an honest job. After a user has gained access to a remote system, *authorization* is a way to restrict operations that the user can perform by the use of system password design by the system administrator to restrict user to some information of the system (Ken Thompson, 2009).

Another security threat came from zombies- computers that had been surreptitiously taken over by hackers to respond to commands via the Internet. Groups of such machines (popularly called zombie armies, or botnets) were being used to send spam (unwanted commercial e-mail) or launch denial-of-service attacks (computerized attacks in which a Web site is bombarded with data that paralyze it). Denial-of-service attacks often were intended to force Web-site owners to pay protection fees to the hackers (Kelvin Bearver, 2006).

Design of Trapdoor for Password Access System

This system is designed to perform at the level of knowledgeable human experts but can be easily understood and utilized by researchers and the general populace as a valuable tool to assist them in the security of system resources from unauthorized access. In addition, the system is intended to be distributed on CD-ROM for other end users who need system resource security. The design basically follows the hierarchy as presented in figure 1.

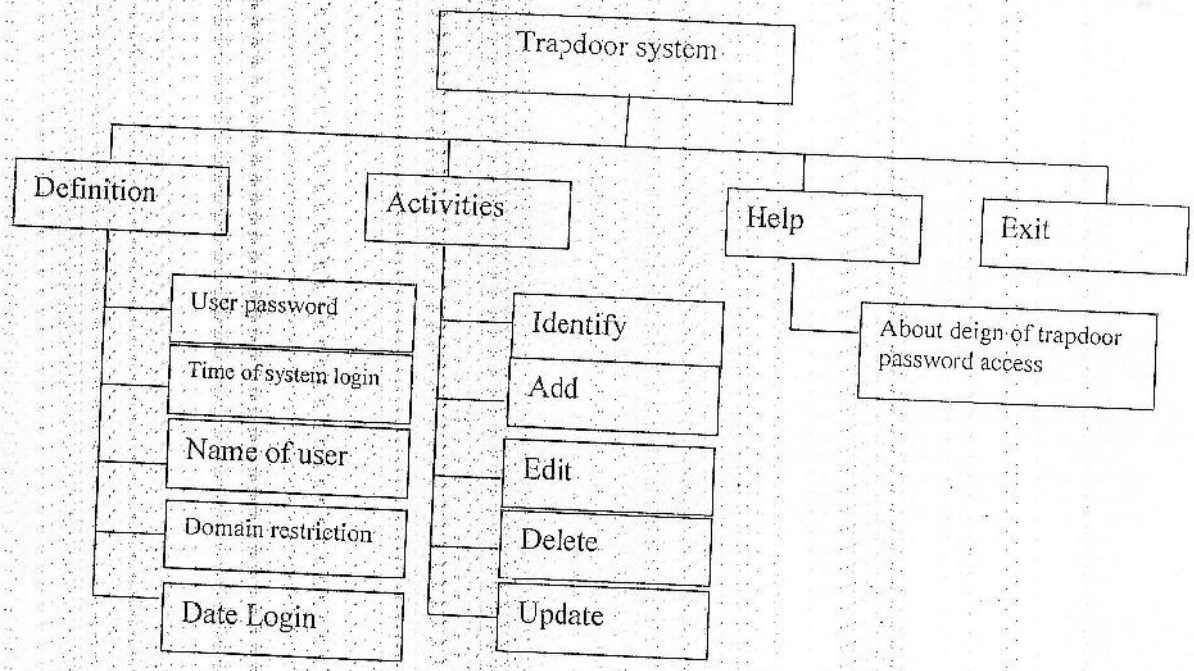


Figure 1: Hierarchical Partition Model of the System.

Knowledge Acquisition

Trapdoor Password access system is mainly based on reasoning methods that reflect human logic skills on security design, hence the password access system was developed based on the identification reasoning process and security knowledge acquired from books, journals, internet, hacking software, students and researchers.

Knowledge Representation

Several informal discussions were conducted with the primary and secondary security system administrator to determine the best strategy for designing the knowledge base trapdoor system. Initially a rule-based, a key for the identification of password based on a series of logical flow between unconventional characters key (semantic nets) and characters (items) were identified as reasonable methods.

User Interface Design

The steps involved in constructing a graphical user interface to direct the user through a smooth access of the system resources was by using non-technical terminologies so that any person having the password to access the trapdoor could easily understand and respond to the on-screen property descriptions. The development of the interface was carried out using Java programming language. The application of Java programming provided a class library for generating interface features such as buttons, windows, pop-up menus, and dialog boxes. The display included a welcome screen, a login screen, etc. The trapdoor system was developed for MS-Windows based computer operating system and can be operated on an Intel-based system with a VGA+ standard color monitor and CD-ROM.

System Design

System design knowledge acquisition involves the validation and verification phases.

i. Validation: Validation of the trapdoor password access of each end user or authorized user access will occur periodically throughout the development of the security system by the researcher. Securing of the system recourses is also collectively review by an accordance of prominent logical skills not directly involved with the design of the trapdoor password access system. Messages from the program will also be review to insure that the system would provide credible security measures. Wrong enter of the password and inconsistencies will be denied from accessing the system except the alternative use of Biometric system.

ii. Verification: Prior to transferring the prototype program to CD-ROM, the trapdoor password system if certified to be correct by the end user or by randomly going through possible pathways and verifying that the conclusion matched the data acquired from the database. Although further verification will be desired, problems of access to the primary security skills, time constraints, hardware incompatibilities and resource limitations prohibited extensive verification.

Input Design

The input design specifies structure which the read data are internally stored. The input design ensures the reliability of the system in producing the desire results. It also determines how efficient the users interact with the Trapdoor Password access system.

The main input of the system is the user response to security question for access displayed on the screen and the system will proceed only if the information required are enter correctly before it load the Domain environment and link to the database.

Input Specification for Trapdoor Password

Table 1 outlines the input specifications of the system.

Table 1.0: Input specification for designed system

Field Name	Data Type	Field Size
User id	Varchar	225
Password	Varchar	225
Time of login	Varchar	15
Domain	Text	225
User Name	Text	225
Date	Varchar	10

Output Design

The most important requirement of an information from the users point of view is the output if produces. If the goal of the user is to get a good output, then if a well design output is not produced at the end, the system will fail to meet user requirement, hence this will no doubt affect the overall effectiveness of the operation of the system, therefore the design of a good output will be based on some consideration made regarding on input and output of the trapdoor system.

Output Specification for Trapdoor Password

a. Access valid
b. Access denied
c. Reenter password
d. Restricted to certain Domain
e. Verified your access by Biometric operation

Program Features

The application is developed with certain features that facilitate the execution of its designed operations. The program feartures are as follows

Log In

This is the first Trapdoor passoward access system which loads my SQL(Structurar Querry Language), the log in fearture is designed to query the database table when any user name and password post back is made and check if the posted entries correspond to any of the registered user name and password in database table. If the entries are validated then the log in features directes the designed system to load the menu bar. See figure 2.

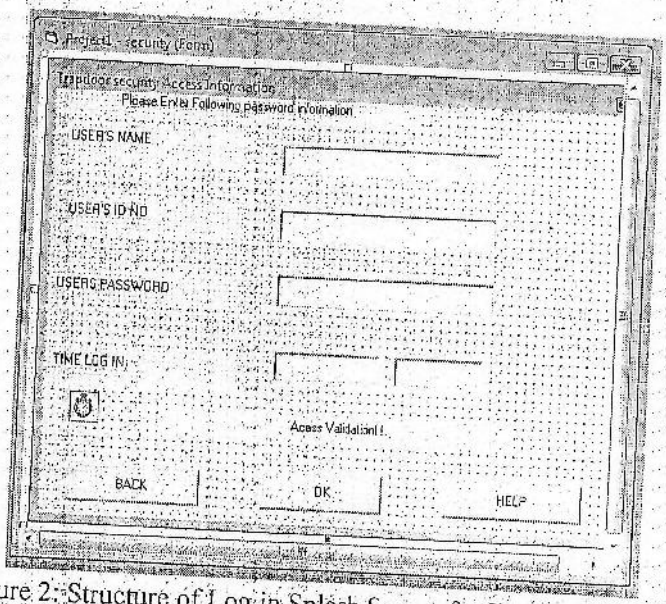


Figure 2: Structure of Log in Splash Screen for Trapdoor System

Menu Form Design

The menu form is element of data which are keyed into the designed to allow for access of the different sub program. Every sub routines are collected by the menu link. Figure 3 shows menu designed frame.

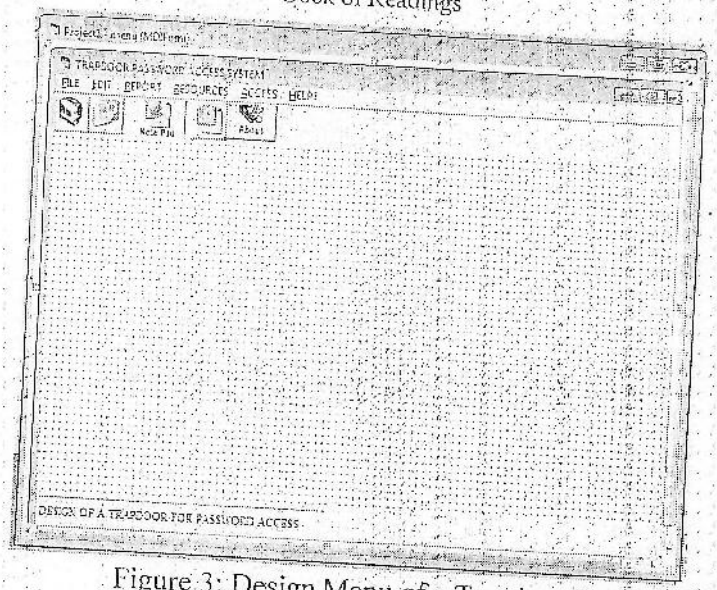


Figure 3: Design Menu of a Trapdoor System

Domain Input Form

The domain input trapdoor form as shown in figure 4 allows authorized users to have access to specific files and folders in the system. Any resource selected by the user is validated from the database to see if the access is allowed to that user and it loads the file or the selected folder.

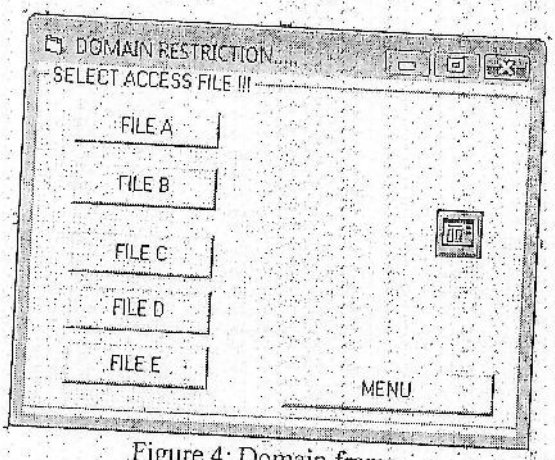


Figure 4: Domain frame

User Access Form

The user access frame allows for validating users access to the data base, allows for editing of authorized users profiles and the administrator user profile. Figure 5 shows the user profile with user Biometric system for easy identification and trapping unauthorized user with another user password and users Id.

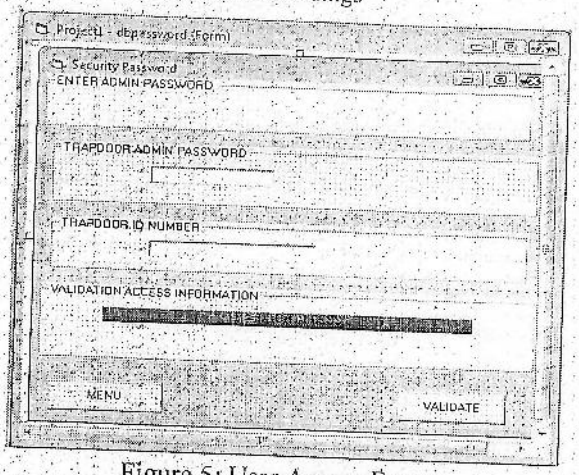


Figure 5: User Access Frame

Creating New User Profile Input Form

In the design of a trapdoor password access security system, the registration of new authorized users is very important. It also enhances administrator monitor the activities that occur in the system database. The interface is as shown in figure 6.

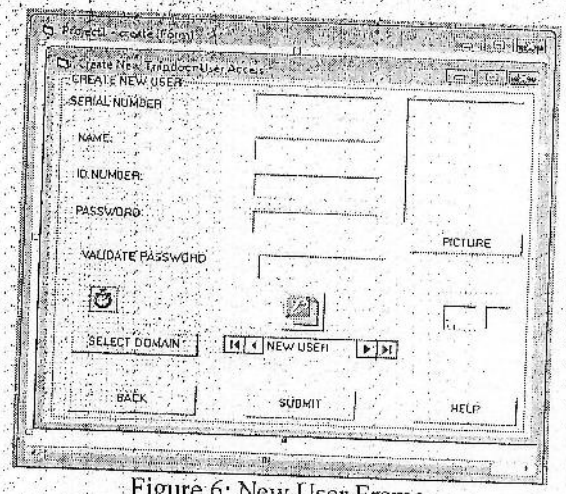


Figure 6: New User Frame

Work Flow Design

The system work flow as illustrated in figure 7 was designed using a selective standard in which the user is asked to enter the password, user identity, time login and domain restriction. The design system requires the user to enter selections by selecting files, folders, documents, and other distinctive areas of the variety. The user then uses his mouse to click a button whose final goal is to generate a single conclusion or a list of possible conclusions that successfully match the resources selected by him. The query activates the search function and rapidly reaches either a specified conclusion, a set of conclusions, or admits it cannot reach a conclusion based on the information provided by the user. In the instance that a conclusion is reached, the list of security resources can be displayed. The user can return to previous menus allowing for multiple access provided the domain is specified by trapdoor administrator sections without exiting or restarting the program.

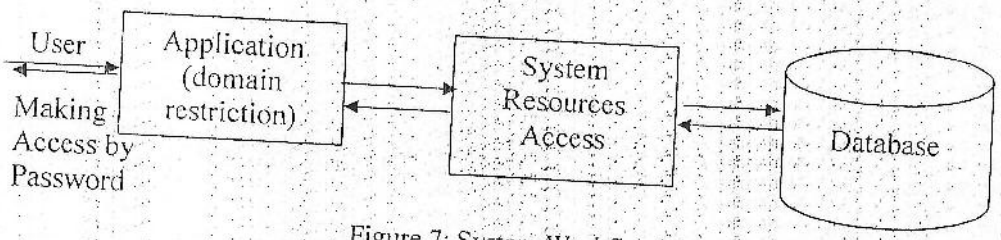


Figure 7: System Workflow.

Module Design

This is used to provide navigations in the program. There are two modules in the program as represented in figure 8 are the main module and the sub module.

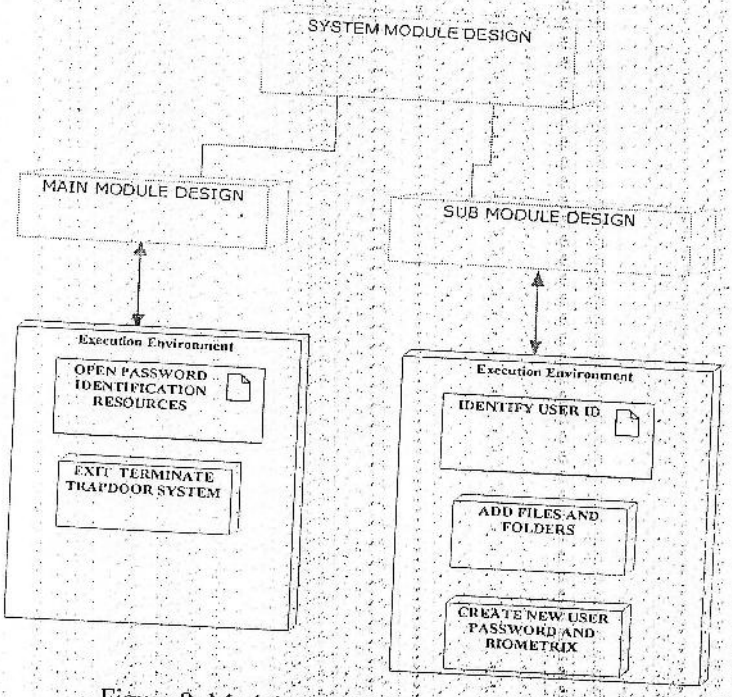


Figure 8: Modular Design Hierarchy

Main Module Design

There are two main modules in the system design, these are: "Open" and "Exit". The "Open" module consists of some sub-modules such as "password identification", "Edit system resources" and "Add files and folders". The "Exit" module is simply used to terminate the application.

Sub-Module Design

There are three sub-modules in the system design. These are "Identify user", used for identifying a particular authorized user access, "Add files and folders", "Create new user access " used for creating user access changing of password into the system and "Edit system resources" which is used to update the existing resources of the system.

Conclusions

The simplicity and accuracy of the new system of Trapdoor password access over the existing system has brought solution to man's limitation and keeping track of unauthorized

users and authorized access as the new system made it possible to store, create, update data base security and Track hacker of system resources.

This project work therefore offers security of data and fast processing of information, thereby saving and researchers from the trouble of unprotected system resources.

Recommendations

Man's limitation and the search for a simplified means of doing task led to the development of the computer and since the new system is more flexible, effective, durable, accurate and efficient, I therefore recommend that the new system (Design of a Trapdoor for Password Access) be put in place to ensure system resources protection.

References

Anderson J. P. and Edwards D. J. "Security Controls for Computer Systems", Technical Report R-609, WH Ware, ed, Feb 1970

Ken Thompson Webopedia (http://www.pcwebopedia.com/) 2009.

Kevin Beaver, Stuart McClure "hacking for dummies" Wiley publishing Inc 2006.

Petersen H. E., Turn R. "System Implications of Information Privacy". *Proceedings of the AFIPS Spring Joint Computer Conference*, vol. 30, pages 291–300. AFIPS Press: 1967

Security Controls for Computer Systems, Technical Report R-609, WH Ware, ed, Feb 1970

Townsend, C. "Mastering Expert Systems with Turbo Prolog". Macmillan, Inc. Indianapolis, IN. 1987