DESIGN AND IMPLEMENTATION OF NETWORK SECURITY (A CASE STUDY OF UBA ENUGU)

BY

NWAUBA NNAEMEKA KENNEDY

CST/T/2010/424

A
PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, CARITAS UNIVERSITY AMORJI – NIKE EMENE ENUGU STATE.

IN

PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF B.SC IN COMPUTER SCIENCE CARITAS UNIVERSITY

JULY, 2013.

APPROVAL

This project has been approved by the department of Computer science, Faculty of Natural Sciences, Caritas University Enugu.

Date _____

_____

MR. TONY UMEASIEGBU

Supervisor

Date _____

_____

DR. ARINZE NWAEZE

Head of Department

Date _____

_____

Dr. B.O.N EKECHUKWU

External Examiner

CERTIFICATION

This is to certify that this project was written in the department of computer Science, faculty of Natural Sciences, Caritas University. I claim the exclusive right and sole authorship of this project work.

NWAUBA NNAEMAKA KENNEDY _____

Name **Signature**

_____

Date

DEDICATION

I dedicate this project to Almighty God for his Loving kindness and mercy, the pillar on which I rest.

I also dedicate this project to my lovely mum for her caring throughout this period of project.

ACKNOWLEDGEMENTS

All thanks and honor is given to God almighty in whose mercy I lived, as he saw me through this year. May his name be praised.

I am using this opportunity to thank all those who in a way contributed immensely to the completion of this project work. My sincere thanks goes to my supervisor Mr. Tony Umeasiegbu for his support, guidance and encouragement during my project writing. I also acknowledge my HOD, DR. ARINZE NWAEZE for his support.

My immeasurable thanks goes to my parents Mr. and Mrs. P.O Nwauba for their love, care, prayers and financial support throughout my stay in school. My God reward them in hundred folds. I am lovely indebted to my lovely sister miss Nwauba Jennifer ,who is not just a sister but a " big sister'', who helped my parents financially to make sure I succeeded.

My profound gratitude also goes to all my course mates, Obinna Kennedy, David Obinna, Okwaraji Uchenna, and my best friend Ujunwa Akuna and others for their advices and little roles they played in today's achievement. I owe a lot of thanks for their enormous contributions, encouragement and time. May God continue to reward u all and keep his eyes over you all Amen.

ABSTRACT

Network Security is essential to any organization. This has been previously done by manual method. But this project is aimed at computerized Network Security to make the work easier. This is possible because of the advance improvement in information technology as pertaining programming language; because this is achieved by the help of visual basic programming language and other programming language. For the first few decades of their existence, computer\ networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem. The requirements of information security within an organization have undergone two major changes in the last several decades before the widespread use of data processing equipment the security of information felt to be valuable to an organization was provided primarily by physical and administrative means with the introduction of computer the need for automated tools for protecting files and other information stored on the computer became an evident .this is especially the case for a shared system such as time sharing system and the need is even more acute for systems that can be accessed for a public telephone or a data network the generic name for the collection of tools to protect data and to thwart hackers is "computer security". Network Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, non repudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Non repudiation deals with signatures.

TABLE OF CONTENT

CHAPTER FOUR

CHAPTER FIVE

CHAPTER ONE

1.0 INTRODUCTION

Several recent proposals have argued for giving third parties and end-users control over routing in the network infrastructure. Some examples of such routing architectures include TRIAD [6], i3 [30], NIRA [39], Data Router [33], and Network Pointers [34]. While exposing control over routing to third-parties departs from conventional network architecture, these proposals have shown that such control significantly increases the flexibility and extensibility of these networks.

Using such control, hosts can achieve many functions that are difficult to achieve in the Internet today. Examples of such functions include mobility, multicast, content routing, and service composition. Another somewhat surprising application is that such control can be used by hosts to protect themselves from packet-level denial-of-service (DOS) attacks [18], since, at the extreme, these hosts can remove the forwarding state that malicious hosts use to forward packets to the hosts. While each of these specific functions can be achieved using a specific mechanism—for example, mobile IP allows host mobility— we believe that these forwarding infrastructures (FIs) provide architectural simplicity and uniformity in providing several functions that makes them worth exploring. Forwarding infrastructures typically provide user control by either allowing source-routing (such as [6], [30], [39]) or allowing users to insert forwarding state in the infrastructure (such as [30], [33], [34]). Allowing

forwarding entries enables functions like mobility and multicast that are hard to achieve using source-routing alone.

While there seems to be a general agreement over the potential benefits of user-controlled routing architectures, the security vulnerabilities that they introduce has been one of the important concerns that has been not addressed fully. The flexibility that the FIs provide allows malicious entities to attack both the FI as well as hosts connected to the FI.

For instance, consider i3 [30], an indirection-based FI which allows hosts to insert forwarding entries of the form (id,R), so that all packets addressed to id are forwarded to R. An attacker A can eavesdrop or subvert the traffic directed to a victim V by inserting a forwarding entry (idV ,A); the attacker can eavesdrop even when it does not have access to the physical links carrying the victim's traffic. Alternatively, consider an FI that provides multicast; an attacker can use such an FI to amplify a flooding attack by replicating a packet several times and directing all the replicas to a victim. These vulnerabilities should come as no surprise; in general, the greater the flexibility of the infrastructure, the harder it is to make it secure.

In this project, we improve the security that flexible communication infrastructures which provide a diverse set of operations (such as packet replication) allow. Our main goal in this project is to show that FIs are no more vulnerable than traditional communication networks (such as IP networks) that do not export control on forwarding. To this end, we present several

mechanisms that make these FIs achieve certain specific security properties, yet retain the essential features and efficiency of their original design. Our main defense technique, which is based on light-weight cryptographic constraints on forwarding entries, prevents several attacks including eavesdropping, loops, and traffic amplification. From earlier work, we leverage some techniques, such as challenge-responses and erasure-coding, to thwart other attacks.

NETWORK SECURITY

(NS) is an important aspect of any system. NETWORK SECURITY is the act of ensuring that an authenticated user accesses only what they are authorized to and no more. The bad news is that security is rarely at the top of people's lists, although mention terms such as data confidentiality, sensitivity, and ownership and they quickly become interested. The good news is that there is a wide range of techniques that you can apply to help secure access to your system. The bad news is that as Mitnick and Simon (2002) point out "…the human factor is the weakest link. Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivette, or ignorance come into play." The go on to say that "security is not a technology problem – it's a people and management problem." Having said that, my experience is that the "technology factor" and the "people factor" go hand in hand; you need to address both issues to succeed.

Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources (such as a movie theater, to which only ticket holders should be admitted), logical resources (a bank account, with a limited number of people authorized to make a withdrawal), or digital resources (for example, a private text document on a computer, which only certain users should be able to read).

Banks are secured financial institutions. They are often housed in large buildings that are located in a commercial or residential area. Banks store money and other financial information and goods.

Money and valuables have been stored in banks since ancient times. As a result of the long history that banks have enjoyed, bank security has also been important for a long time. Some of the oldest banks in the world have the best security available. These banks include the Bank of Sweden, the Bank or England, Bank of America, and Swiss Banking.

Bank security usually includes a staff of security guards, a security system, and one or more vaults. Security guards are uniformed personnel that maintain high visibility and watch cameras and alarms. Cameras and alarms are usually top of the line systems in banks and other financial buildings. But these security elements are not exclusive to banks. Some of these elements can be found in other commercial buildings and even residential homes.

Basic security starts with the locks. For a high level of security, windows and doors will need the best locks. After high quality locks are installed many property owners opt for a security system or even security cameras.

Security cameras are often a small part of a larger security system. Systems often include motion detectors, alarms, sensors, and cameras. Cameras are arguably the most important because they allow the property owner to see and record everything that happens in and around their building or property.

Cameras can be installed by a professional or by a property owner. For a large and elaborate system it may be best for a professional to do the work. But for a smaller and easy layout, a property owner should have no problem installing a system by following the manufactures instructions. If he does than there is usually a local installer that can be called to help finish the job.

1.1 STATEMENT OF THE PROBLEM

Owing to:

1. Fraudulent act of some customer/workers
2. Accessing the organizational data/information unauthorized
3. Sensitive nature of bank data/information
4. Valuable or costly items in bank

5. Increase in crime in our society

The need arise for the development of computerized NETWORK SECURITY to eliminate such problems.

1.2 PURPOSE OF STUDY

The main purpose of this project is to design a NETWORK SECURITY that will assist UBA in the area of ensuring effective security measures.

1.3 AIMS AND OBJECTIVES

This project will have the following aims and objectives:

- Detecting security violations
- Re-creating security incidents
- To disallow unauthorized users
- To safeguard the organizational data/information
- To computerized the organizational security
- To enhance the organizational security
- To eliminate all forms of mistakes associated with security control

1.4 SCOPE OF STUDY

This research work will access the design and implementation of NETWORK SECURITY in UBA Enugu. It will look into the operations of this bank in the aspect of computerizing their security control system.

1.5 CONSTRAINTS

This project will be limited to the data available at hand, data outside the researcher will not be made use of.

The limitations militating against this research are financial constraints, time factor and other circumstances.

1.6 ASSUMPTIONS

Accuracy, efficiency and reliability is associated with Network Security.

For the purpose of this research, my assumptions can be stated as follows:

1. The application of computer related garget for security control
2. A computerized Network Security is effective and dependable

1.7 DEFINITION OF TERMS

Administration is an aspect of running the organization by devising systems which will run smoothly.

2. **Client:** This any process that request specific services from server processes.

3. Computer: This is an electrons machine that can accept; handle and manipulate data by performing arithmetic and logic operations without human intervention usually under the control of programmes.

4. **Data:** This is fore runner of information. It is unprocessed fact.

5. Database is a collection of information that is related to a particular subject or purpose.

6. **Hardware:** This is the electromechanical part of computer system.

7. **Information:** This is data that have been processed, interpreted and understood by the recipient of the message or report.

8. Internet is a collection of computer networks that operate to common standards and enable the computes and the program they run to communicate directly.

9. **Server:** This is a process that provides requested services for clients.

10. **Software:** This is a logically written program that hardware uses to perform it's operation.

11. System is the collection of hardware, software, data information, procedures and people.

12. Website is a space or location customized by a company, organization or an individual which is locatable within an address on the internet.

CHAPTER TWO

2.0 LITERATURE REVIEW

According to John J. Murphy, Technical Analysis of the Financial Markets Authentication is the act of determining the identity of a user and of the host that they are using. The goal of authentication is to first verify that the user, either a person or system, which is attempting to interact with your system is allowed to do so. The second goal of authentication is to gather information regarding the way that the user is accessing your system. For example, a stock broker should not be able to make financial transactions during off hours from an Internet café, although they should be able to do so from their secured workstation at their office. Therefore gathering basic host information, such as its location and security aspects of its connection (is it encrypted, is it via a physical line, is the connection private, …), is critical.

There are several strategies that you can follow to identify a client:

- User id and password. This is the most common, and typically the simplest, approach to identifying someone because it is fully software-based.

- Physical security device. A physical device, such as a bank card, a smart card, or a computer chip (such as the "Speed Pass" key chains used by gas stations) is used to identify a person. Sometimes a password or

personal identification number (PIN) is also required to ensure that it is the right person.

- Biometric identification. Biometrics is the science of identifying someone from physical characteristics. This includes technologies such as voice verification, a retinal scan, palm identification, and thumbprints.

According to McKay, Peter A, A , Authorization is the act of determining the level of access that an authorized user has to behavior and data. This section explores the issues surrounding authorization, there is often more to it than meets the eye, and then explores various database and object-oriented implementation strategies and their implications.

Issues.

Fundamentally, to set an effective approach to authorization the first question that you need to address is "what will we control access to?" My experience is that you can secure access to both data and functionality, such as access to quarterly sales figures and the ability to fire another employee respectively. Your stakeholders' requirements will drive the answer to this question. However, the granularity of access, and your ability to implement it effectively, is a significant constraint. For example, although you may be asked to control access to specific columns of specific rows within a database based on complex business rules you may not be able to implement this in a cost effective manner that also conforms to performance constraints.

The second question that you need to answer is "what rules are applicable?" The answer to this question is also driven by your stakeholders' requirements; although you may need to explore various security factors that they may not be aware of (they're not security experts after all). These factors, which are often combined, include:

- Connection type.
- Update access.
- Time of day.
- Existence.
- Cascading authorization.
- Global permissions.
- Combination of privileges.

Database Implementation Strategies

Let's start by reviewing the concepts of roles and security contexts. A role is a named collection of privileges (permissions) that can be associated to a user. So, instead of managing the authorization rights of each individual user you instead define roles such as HR_ Manager, HR_ User, Manufacturing Engineer, Accountant, and so on and define what each role can access. You then assign users to the roles, so Sally Jones and her co-workers would be associated with

the role of Manufacturing Engineer. Someone else could be assigned the roles of HR_ Manager and HR_ User if appropriate. The use of roles is a generic concept that is used by a wide range of technologies, not just databases, to simplify the security administration effort.

A security context is the collection of roles that a user is associated with. The security context is often defined as part of the authentication process. Depending on the technology used a security context is maintained by the system, this is very common in GUI applications, or must be passed around by the system, something that is common with browser-based n-tier system. A combination of the two strategies is also common.

Authorization can be enforced within your database by a variety of means (which can be combined). These techniques include:

- Permissions. Permission is a privilege or authorization right, that a user or role has regarding an element (such as a column, table, or even the database itself). A permission defines the type of access that that is permitted, such as the ability to update a table or to run a stored procedure. In SQL, permissions are given via the GRANT command and removed via the REVOKE command. When a user attempts to interact with a database his or her permissions are checked, and if the user is not authorized to perform part of the interaction, which could be a transaction, the interaction fails and an error is returned.

- Views. You can control, often to a very fine level, the data that a user can access via the use of views. This is a two-step process. First, you define views that restrict the tables, columns, and rows within the tables that a role can access. Second, you define permissions on those views.

- Stored procedures. Code within the stored procedure can be written to programmatically check security access rules.

- Proprietary approaches. A new option being offered by some database vendors is proprietary security tools. One example is Oracle Label Security, an add-on that enables you to define and enforce row-level permissions.

The primary goal of database security is to ensure that there isn't any "backdoor" ways to access critical corporate data. Many organizations choose to disallow ad-hoc queries to production databases to help minimize the chance of unauthorized access (as well as to avoid the associated performance problems). Many organizations introduce reporting databases such as data marts to support ad-hoc queries. According to Gregory J. Millman on his book titled Access Control System Operation, when a credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transition log to a database. When access is denied based

on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room but Bob does not. Alice either gives Bob her credential or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted. The second factor can be a PIN, a second credential, operator intervention, or a biometric input. Often the factors are characterized as

- something you have, such as a credential,
- Something you know, e.g. a PIN.

CHAPTER THREE

3.0 DESCRPTION AND ANALYSIS OF THE EXISTING SYSTEM

The existing system of Network Security maintained by UBA Enugu is a manual system. There have been a lot of lapses concerning the operations involved in the computerized Network Security.

One of the primary roles of Network Security is to satisfy the needs of customers and the organization thereby maximizing profit.

3.1 FACT FINDING METHOD USED

The researcher used the following method of data collection in writing the project.

a. Interview method: People that deal on computerized Network Security where interviewed to share their opinion concerning the manual method.

b. Written Document: A lot of documents concerning computerized Network Security where studied from which I gather useful information for the project.

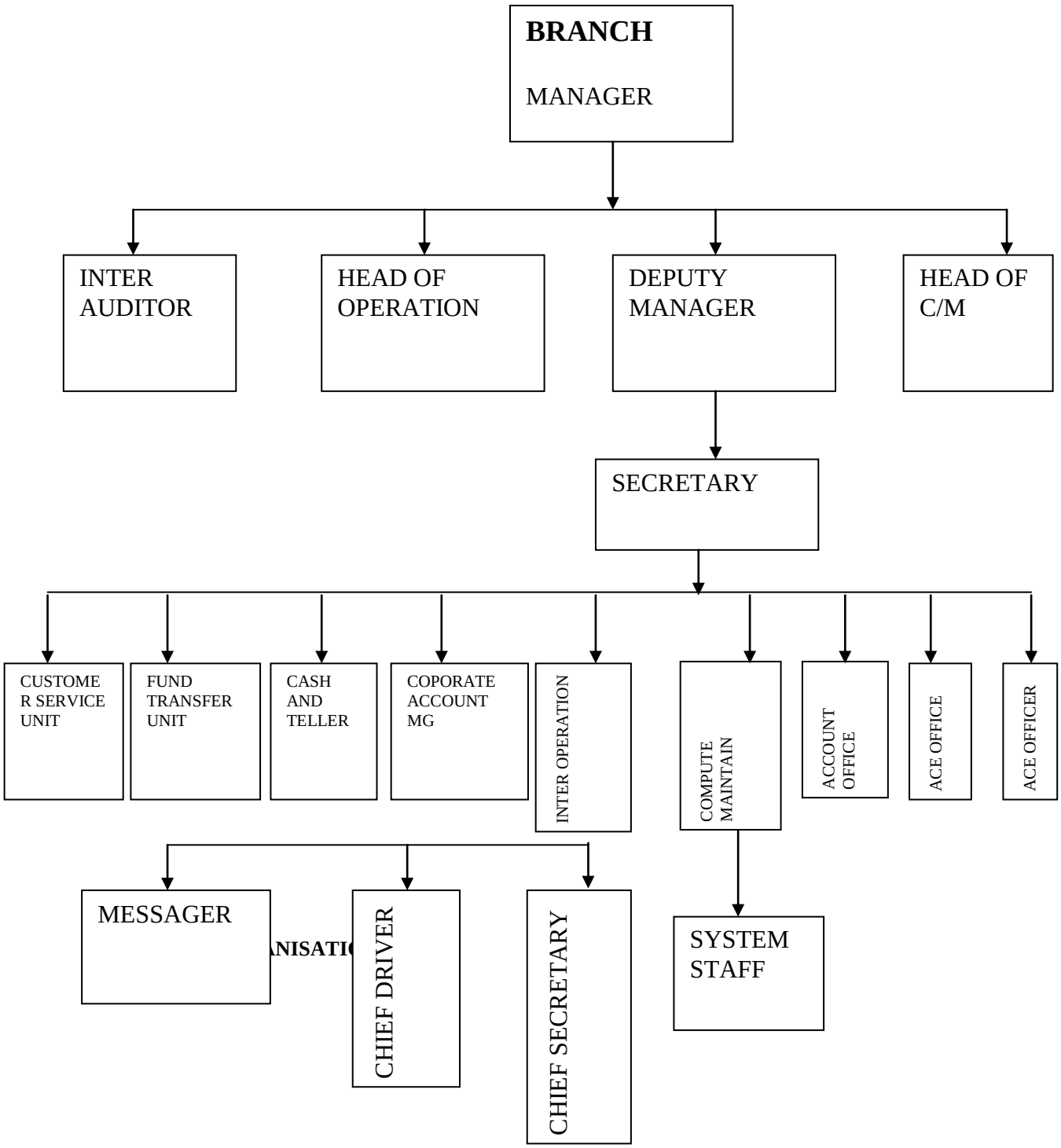
c. Observation: Observation method was also used to get information concerning the project.

3.2 OBJECTIVES OF THE EXISTING SYSTEM

The main objectives of the existing include:

1. To eliminate all forms of mistakes associated with security control
2. Detecting security violations
3. Re-creating security incidents
4. To disallow unauthorized users
5. To safeguard the organizational data/information
6. To computerized the organizational security
7. To enhance the organizational security

3.3 ORGANISATION CHART



3.4 INPUT/PROCESS/OUTPUT ANALYSIS

INPUT ANALYSIS

Since the major activity carried out by the computerized NETWORK SECURITY management is the changing of currency to customers, the following are the requirements of this management from their customers.

User log-in Account

User Name

Password

Retype Password

NAME

ACCOUNT NO

TYPE OF CURRENCY

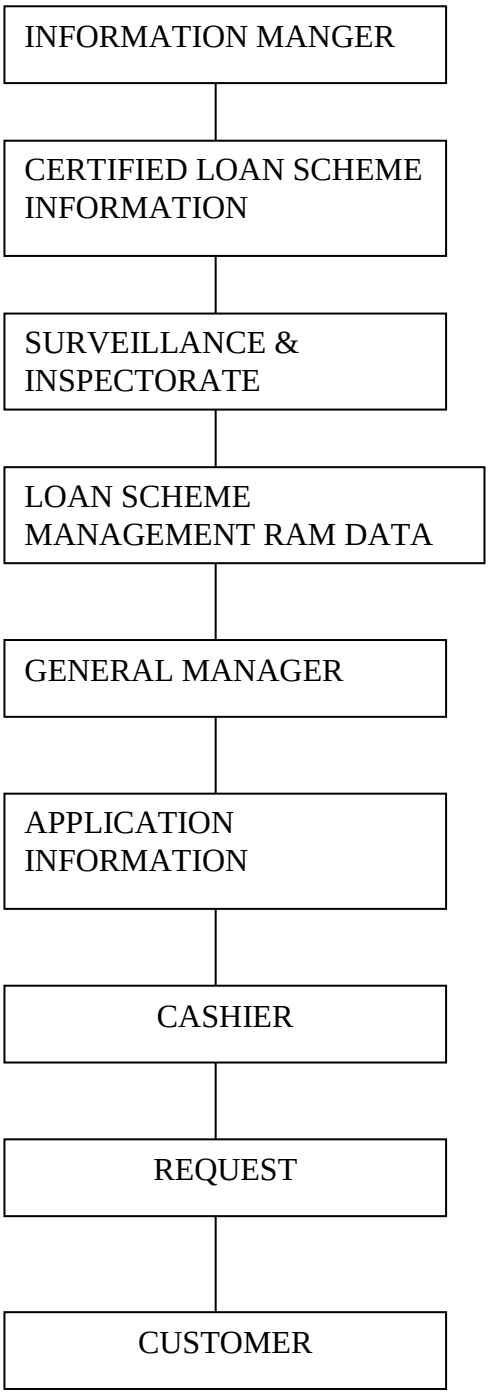
DATE OF TRANNSTION

PROCESS ANALYSIS

All the input specifications are put into consideration and specification of authenticity carried out before an activity is accomplished.

Necessary signatures are signed and clarified without any waste of time. At the end, accuracy is achieved and loopholes does not abound.

3.5 INFORMATION FLOW DIAGRAM



CHAPTER FOUR

4.0 DESIGN OF A NEW SYSTEM

The design of the new system is born out of the report from the analysis of the existing system. The new system is automatic in operation and its features are represented in computer coding formats under this chapter.

4.1 OUTPUT SPECIFICATION AND DESIGN

The output specification includes:

User Name

Password

Retype Password

NAME

ACCOUNT NO

TYPE OF CURRENCY

DATE OF TRANNSTION

4.2 INPUT SPECIFICATION AND DESIGN

THE INPUT ELEMENTS ARE

S/N	FIELD NAME	FIELD VARIABLE	FIELD WIDTH	FIELD TYPE
	USERNAME PASSWORD RETYPE PASSWORD ACCOUNT NO DATE OF TRANNSTION NAME	UN P RP AN DOT N	20 15 20 16 10 15	TEXT TEXT TEXT NUMBER NUMBER TEXT

USER LOG-IN FORM

User Name: _____

Password _____

Retype _____

User Name_____ Retype Password_____

NAME ACCOUNT NO_____ TYPE OF CURRENCY_____

DATE OF TRANNSTION_____

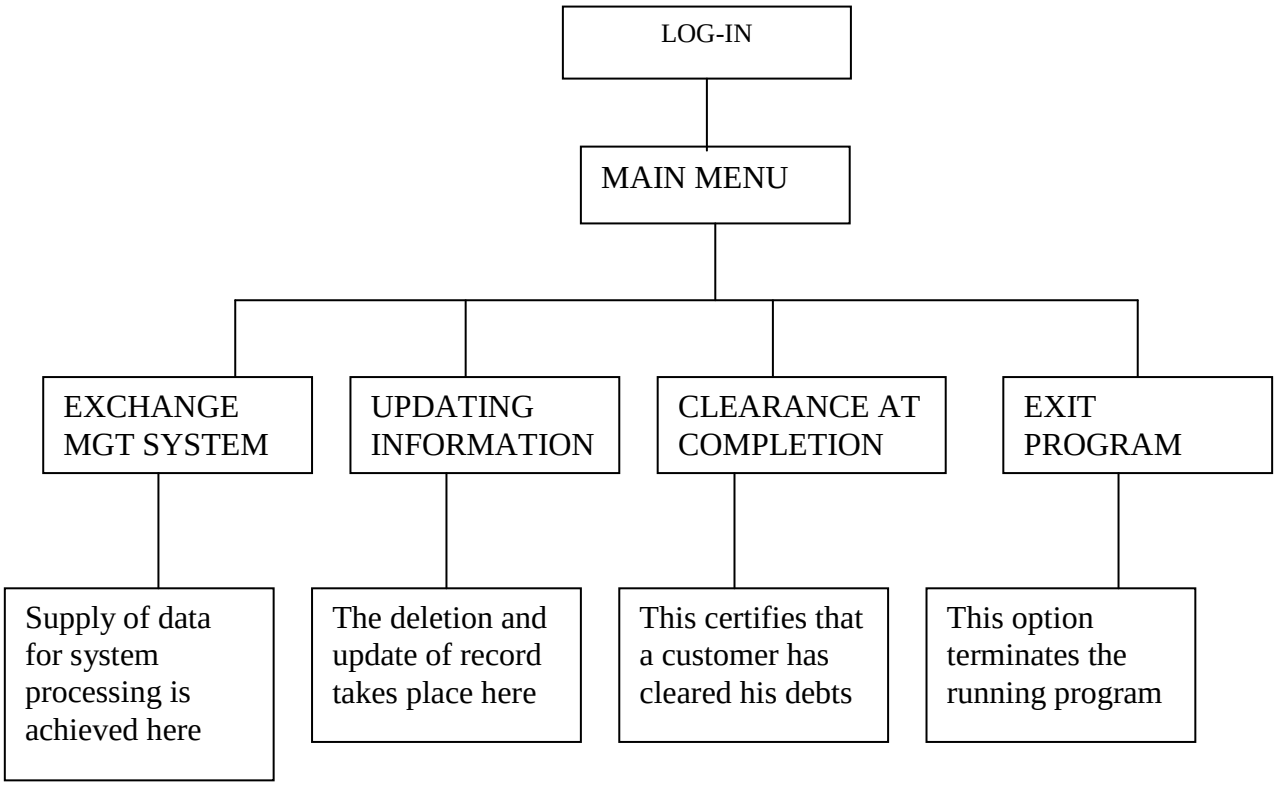
4.3 FILE DESIGN

NAME _____ACCOUNT NO _____

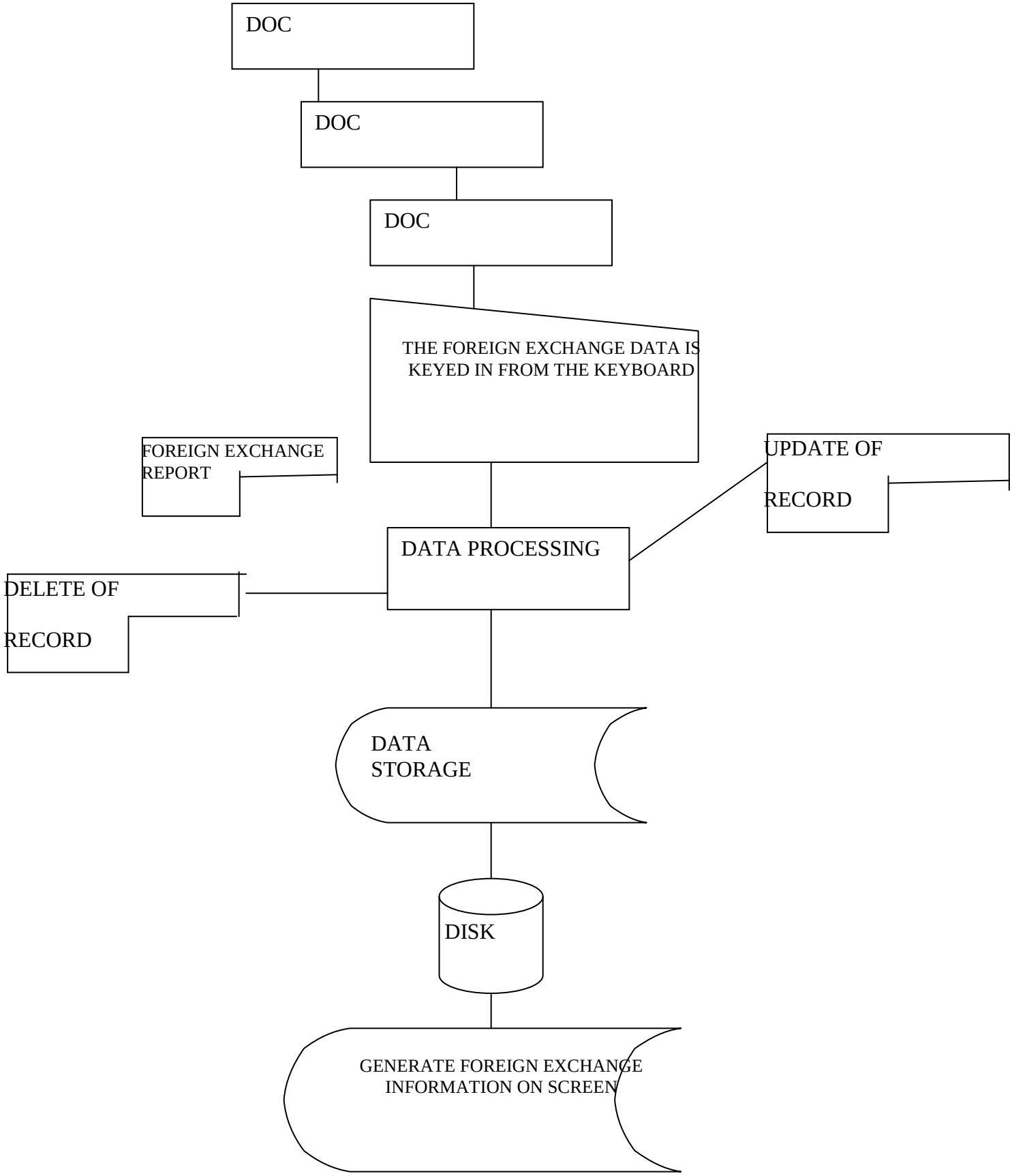
TYPE OF CURRENCY _____AMOUNT TO CHANGE _____

DATE OF TRANNSTION _____

4.4 PROCEDURE CHART



4.5 SYSTEM FLOWCHART



45.1 SYSTEM REQUIREMENTS

HARDWARE REQUIREMETNS

MODEL - 550

STORAGE - 10GB

MEMORY - 128MB

DISPLAY - 15” SVGA

DRIVE – 31/2 FDD

PRINTER - DESIGN PRINTER

SOFTWARE REQUIREMENTS

OPERATING SYSTEM – WINDOW XP

LANGUAGE - VISAUL BASIC

ANT – VIRUS - AVASTA

CHAPTER FIVE

5.0 IMPLEMENTATION

The computer needs to understand the design of the new system for its effective operations and use. The design has to be coded in computer understandable formats. The structures are designed under this chapter.

5.1 PROGRAM DESIGN

The programming is made under modules which are:

FILE ORGANIZATION MODULE

This module handles data entry and storage. It consists of data entry screen which is the medium through which data is entered into the computer system. The data received is stored automatically by commanding the computer to save.

INFORMATION UPDATA MODLE

The information update module makes it possible for modification to be effected on already maintained record. This module makes the system to be flexible and reliable.

INFORMATION REQUIREMENT MODULE

Accurate report generation is made possible through this module, the comprehensive report of the system under this module. The particular report generator depends on the user's request.

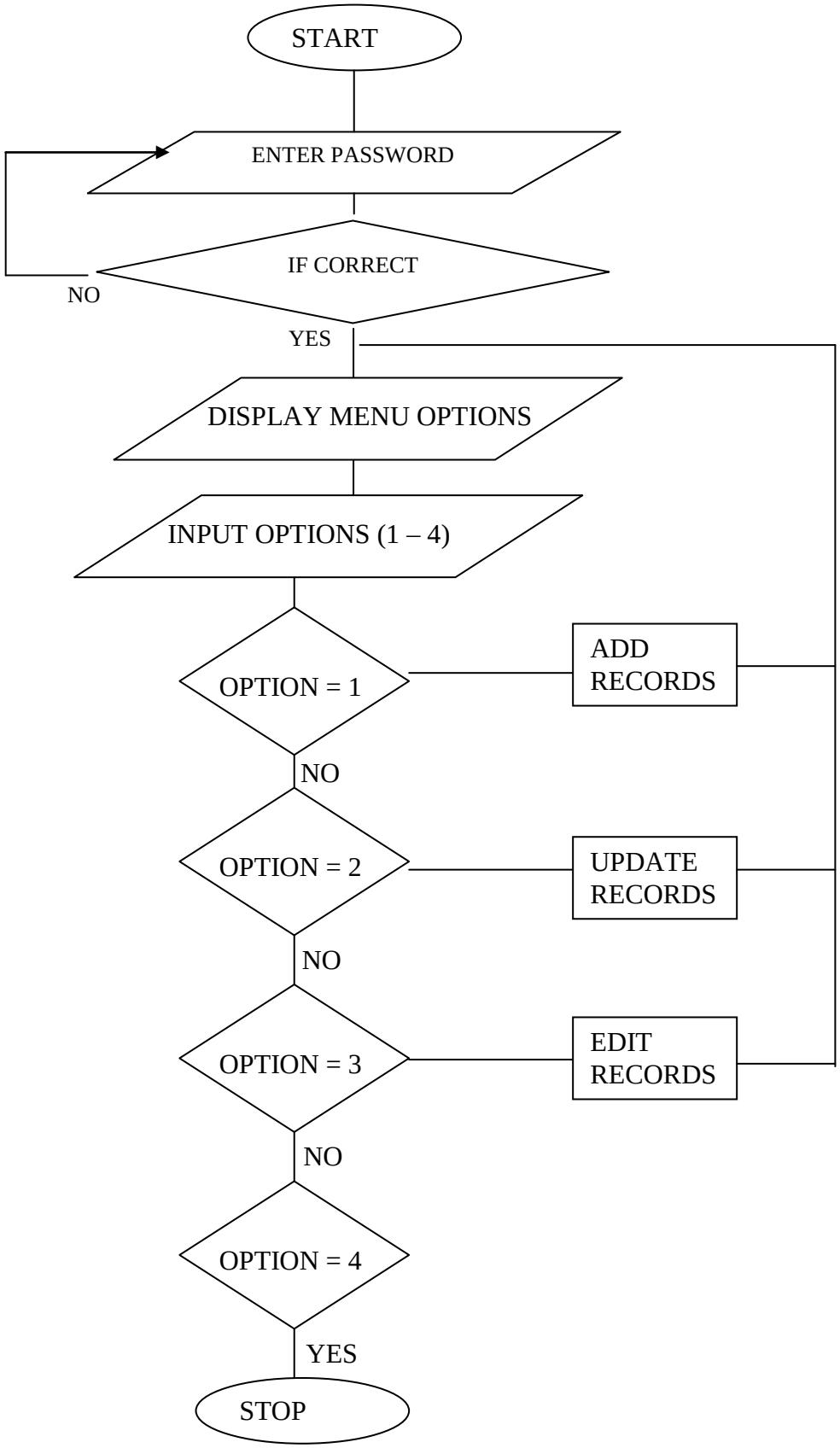
PROCESSING MODLE

This module carries out action on the supplied data in order to achieve the best desired result.

EXIT MODULE

This module terminates the running of the program.

5.2 PROGRAM FLOWCHART



5.3 DOCUMENTATION

This project is divided into five chapters. Chapter one consists of the introduction, purpose of study, aims and objectives, scope, constraints, assumptions and definition of terms.

Chapter two is literature review while chapter three is the description and analysis of the existing system which is made up of organizational chart, objectives, methods of data collection, input/process/output, information flow diagram and justification.

Chapter four is the design of a new system. It contains the output specification, input specification and file design, flowchart and system requirements.

Chapter five is implementation which consists of program design, program flowchart, pseudo codes, source program, test run

Documentation, summary, recommendation and conclusion.

PROGRAM HELP MENU

This program was coded in a programming language called VISUAL BASIC. The program is run through Window into the VBASIC directory. There, it is expected that laying in the program and pressing F5, one can view the NETWORK SECURITY system as done in UBA Enugu. Clicking exist on the file menu will quit the program. The file name for the program is FOREIGN EXCHANGE program

5.4 RECOMMENDATION & CONCLUSION

5.5 RECOMMENDATION

This great research is recommended to individuals who are involved in one business transaction or the other, that they continue to fulfill their motives by making profit through NETWORK SECURITY.

5.6 CONCLUSION

In computer security, access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems.

In any access control model, the entities that can perform actions in the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects (see also Access Control Matrix). Subjects and objects should both be considered as software entities, rather than as human users: any human user can only have an effect on the system via the software entities that they control. Although some systems equate subjects with user IDs, so that all processes started by a user by default have the same authority, this level of control is not fine-grained enough to satisfy the Principle of least privilege, and arguably is responsible for the prevalence of malware in such systems (see computer insecurity).

In some models, for example the object-capability model, any software entity can potentially act as both a subject and object.

Access control models used by current systems tend to fall into one of two classes: those based on capabilities and those based on access control lists (ACLs). In a capability-based model, holding an unforgivable reference or capability to an object provides access to the object (roughly analogous to how possession of your house key grants you access to your house); access is conveyed to another party by transmitting such a capability over a secure channel. In an ACL-based model, a subject's access to an object depends on whether its identity is on a list associated with the object (roughly analogous to how a bouncer at a private party would check your ID to see if your name is on the guest list); access is conveyed by editing the list. (Different ACL systems have a variety of different conventions regarding who or what is responsible for editing the list and how it is edited.)

Both capability-based and ACL-based models have mechanisms to allow access rights to be granted to all members of a group of subjects (often the group is itself modeled as a subject).

Access control systems provide the essential services of identification and authentication (I&A), authorization, and accountability where:

- identification and authentication determine who can log on to a system, and the association of users with the software subjects that they are able to control as a result of logging in;
- authorization determines what a subject can do;
- Accountability identifies what a subject (or all subjects associated with a user) did.

5.7 SUMMARY

Routing is one of the most important parts of the infrastructure that keeps a network running, and as such, it is absolutely critical to take the necessary measures to secure it. There are different ways routing can be compromised, from the injection of illegitimate updates to DOS specially designed to disrupt routing. Attacks may target the router devices, the peering sessions, and/or the routing information. Fortunately, protocols like BGP, IS-IS, OSPF, EIGRP and RIPv2 provide a set of tools that help secure the routing infrastructure. This section provides the guidelines for using such tools.

The router's primary functions are to learn and propagate route information, and ultimately to forward packets via the most appropriate paths. Successful attacks

against routers are those able affect or disrupt one or more of those primary functions by compromising the router itself, its peering sessions, and/or the routing information.

Routers are subject to the same sort of attacks designed to compromise hosts and servers, such as password cracking, privilege escalation, buffer overflows, and even social engineering. Most of the best practices in this document help mitigate and even prevent some of those threats.

Peering relationships are also target of attacks. For most routing protocols routers cannot exchange route information unless they establish a peering relationship, also called neighbor adjacency. Some attacks attempt to break established sessions by sending the router malformed packets, resetting TCP connections, consuming the router resources, etc. Attacks may also prevent neighbor adjacencies from being formed by saturating queues, memory, CPU and other router resources. This section of the document presents a series of best practices to protect neighbor adjacencies from those threats.

Finally, routing can also be compromised by the injection of false route information, and by the modification or removal of legitimate route information. Route information can be injected or altered by many means, ranging from the insertion of individual false route updates to the installation of bogus routers into the routing infrastructure. Potential denial of service conditions may result from intentional loops or black-holes for particular destinations. Attackers may

also attempt to redirect traffic along insecure paths to intercept and modify user's data, or simply to circumvent security controls. This section also includes a collection of best practices designed to prevent the compromising of routing information.

REFERENCES

Anderson, A.C. (2006). *Cryptography and network security.* New York: A Bantam Press.

Applied cryptography. (2001). *Computer security.* U.S.A: CRC Press.

Apostolou, B. (2000). *Internal fraud Investigation.* Louis Avenue: Institute of Internal Auditor's Publication.

A.C.F.E. (2002). *Report on fraud Occurrence*. http: www.wikipedia.com

Boyle, L., & Panko, H. (2009). *Corporate Computer Security*. America: Bank of Settlement.

Bishop, A.A. (2011). *Threats Security*. France: Art and Science.

Bytes (2011). *Security tool*. http://www. Securebytes.com

Chukwu, L.C. (2010). *Securing and Investigation*. Owerri: Benson Publication.

Casey, E. (2010). *Handbook of Investigation.* U.S.A: Academic Press Publication.

Chandelle, V. (2001). *Anomaly detection.* India: University of Minnesota Publication.

Howard, L., & Leblanc, K. (2002). *Writing Secure code*. U.S.A: Editing Microsoft Press.

John, J. (2001). *A Triennial Central Bank survey*. London: Bank for International Settlements.

Simmons, A. (December 2010). *Ontology for Network Security Attack.* Lecture note in Computer science.

Solomon, P.O. (November 2000). *Encrypting Messages*. Russia: Encrypting Messages Centre.

APPENDIX I

PSEUDOCODE

Press F5 to run the program. Press any key to continue.

1. Enter password
2. initialize variables
3. input data records
4. is data ok
5. if yes write data to disk
6. add more variables
7. if yes repeats step 1
8. end

EDIT RECORD

1. Enter record No to Edit
2. Does record exist
3. If yes then edit record
4. Edit another record
5. If yes then repeat step 1
6. End

DELETE RECORD

1. Enter record No to delete
2. Does record exist
3. If yes then update database
4. End if
5. Delete another
6. If yes then repeat step 1
7. Stop

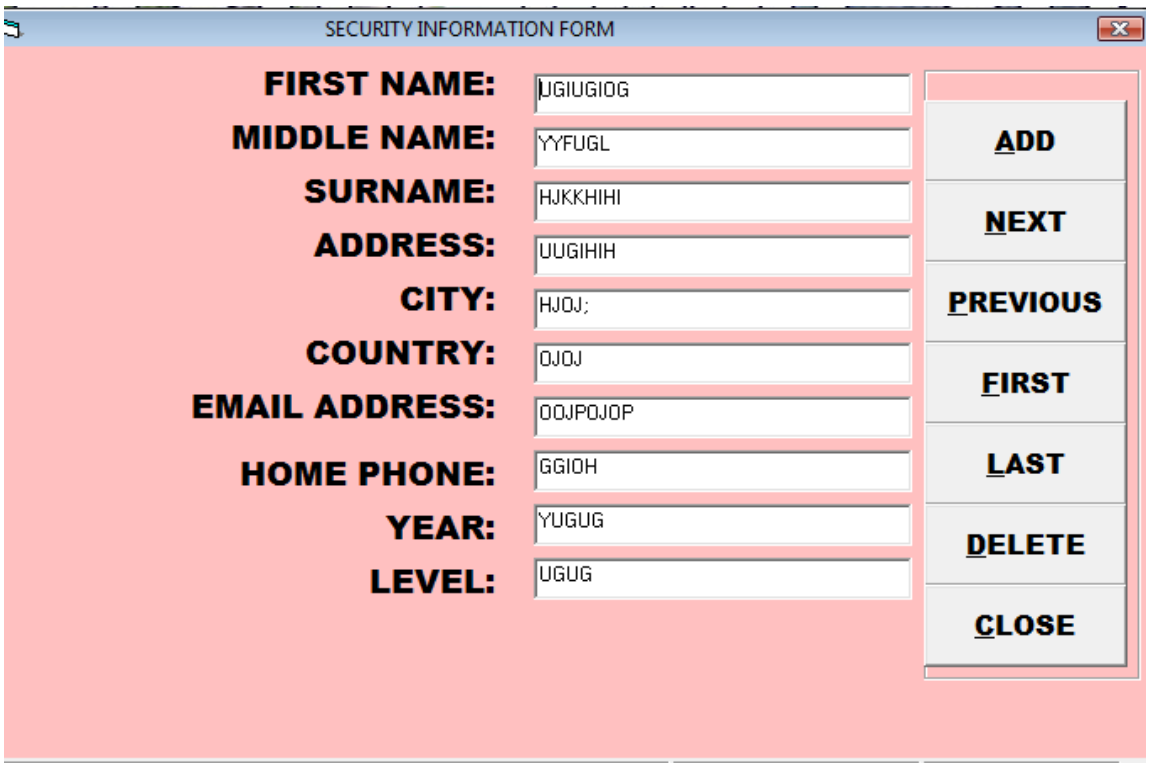
APPENDIX II
SOURCE LISTING

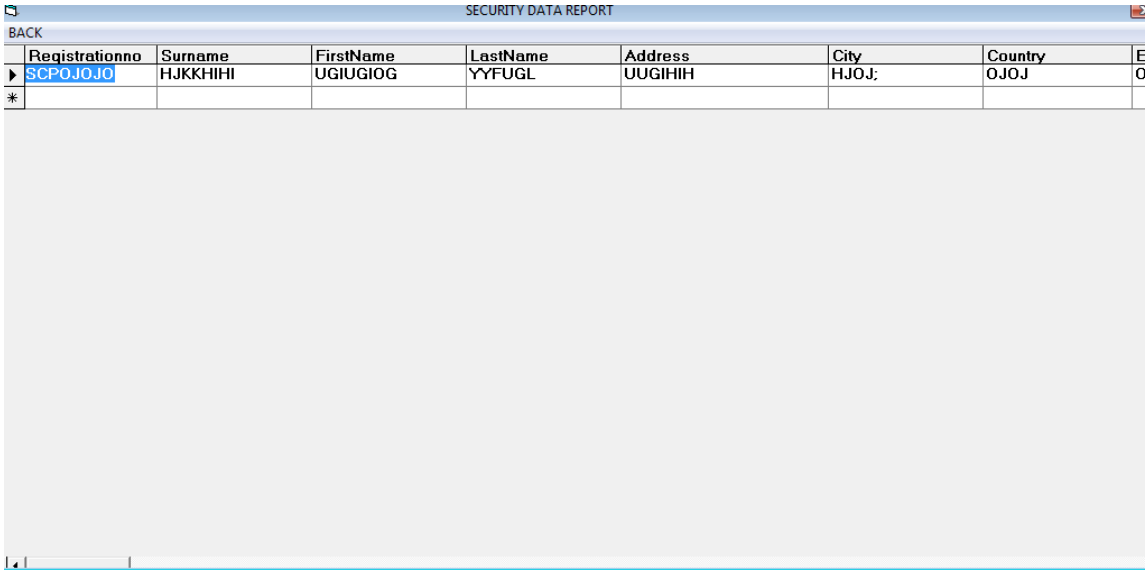
```
VERSION 5.00
Object = "{831FDD16-0C5C-11D2-A9FC-0000F8754DA1}#2.0#0"; "MSCOMCTL.OCX"
Begin VB.Form main
   BackColor       =   &H00004000&
   BorderStyle     =   1  'Fixed Single
   Caption         =   "NETWORK SECURITY INFORMATION SYSTEM"
   ClientHeight    =   7515
   ClientLeft      =   45
   ClientTop       =   345
   ClientWidth     =   10080
   LinkTopic       =   "Form1"
   MaxButton       =   0   'False
   MinButton       =   0   'False
   ScaleHeight     =   7515
   ScaleWidth      =   10080
   StartUpPosition =   2  'CenterScreen
   Begin MSComctlLib.StatusBar StatusBar1
      Align           =   2  'Align Bottom
      Height          =   375
      Left            =   0
      TabIndex        =   4
      Top             =   7140
      Width           =   10080
      _ExtentX        =   17780
      _ExtentY        =   661
      _Version        =   393216
      BeginProperty Panels {8E3867A5-8586-11D1-B16A-00C0F0283628}
         NumPanels       =   3
         BeginProperty Panel1 {8E3867AB-8586-11D1-B16A-00C0F0283628}
            Object.Width          =   10583
            MinWidth        =   10583
            Text            =   "HYPERDLINK TECHNOLOGY"
            TextSave        =   "HYPERDLINK TECHNOLOGY"
         EndProperty
         BeginProperty Panel2 {8E3867AB-8586-11D1-B16A-00C0F0283628}
            Style           =   6
            Object.Width          =   3919
            MinWidth        =   3919
            TextSave        =   "2/18/2011"
         EndProperty
         BeginProperty Panel3 {8E3867AB-8586-11D1-B16A-00C0F0283628}
            Style           =   5
            Alignment       =   2
            Object.Width          =   3134
            MinWidth        =   3134
            TextSave        =   "3:58 AM"
         EndProperty
      EndProperty
      MousePointer    =   3
      BeginProperty Font {0BE35203-8F91-11CE-9DE3-00AA004BB851}
         Name            =   "Arial Black"
         Size            =   9.75
         Charset         =   0
         Weight          =   900
         Underline       =   0   'False
         Italic          =   -1  'True
```

```
      Strikethrough   =   0   'False
    EndProperty
  End
  Begin VB.Image Image1
    Height          =   4815
    Left            =   0
    Picture         =   "main.frx":0000
    Stretch         =   -1  'True
    Top             =   2400
    Width           =   10095
  End
  Begin VB.Label Label5
    Alignment       =   2  'Center
    BackColor       =   &H00004000&
    Caption         =   "HELP"
    BeginProperty Font
      Name          =   "Arial Black"
      Size          =   30
      Charset       =   0
      Weight        =   900
      Underline     =   0   'False
      Italic        =   0   'False
      Strikethrough   =   0   'False
    EndProperty
    ForeColor       =   &H0000C0C0&
    Height          =   975
    Left            =   7320
    MousePointer    =   8  'Size NW SE
    TabIndex        =   3
    Top             =   120
    Width           =   2535
  End
  Begin VB.Label Label4
    Alignment       =   2  'Center
    BackColor       =   &H00004000&
    Caption         =   "SECURITY REPORT"
    BeginProperty Font
      Name          =   "Arial Black"
      Size          =   30
      Charset       =   0
      Weight        =   900
      Underline     =   0   'False
      Italic        =   0   'False
      Strikethrough   =   0   'False
    EndProperty
    ForeColor       =   &H0000C0C0&
    Height          =   1695
    Left            =   3600
    TabIndex        =   2
    Top             =   120
    Width           =   3495
  End
  Begin VB.Label Label3
    Alignment       =   2  'Center
    BackColor       =   &H00004000&
    Caption         =   "EXIT"
    BeginProperty Font
      Name          =   "Arial Black"
      Size          =   36
      Charset       =   0
```

```
      Weight         =   900
      Underline      =   0   'False
      Italic         =   0   'False
      Strikethrough  =   0   'False
    EndProperty
    ForeColor      =   &H0000C0C0&
    Height         =   855
    Left           =   7560
    TabIndex       =   1
    Top            =   1200
    Width          =   2055
  End
  Begin VB.Label Label1
    Alignment      =   2  'Center
    BackColor      =   &H00004000&
    Caption        =   "SECURITY FORM"
    BeginProperty Font
      Name           =   "Arial Black"
      Size           =   30
      Charset        =   0
      Weight         =   900
      Underline      =   0   'False
      Italic         =   0   'False
      Strikethrough  =   0   'False
    EndProperty
    ForeColor      =   &H0000C0C0&
    Height         =   1695
    Left           =   0
    TabIndex       =   0
    Top            =   0
    Width          =   3495
  End
End
Attribute VB_Name = "main"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = False


Private Sub Label1_Click()
wordgame.Show
Me.Hide

End Sub

Private Sub Label1_MouseMove(Button As Integer, Shift As Integer, X As Single, Y As Single)
Label1.ForeColor = vbWhite

End Sub

Private Sub Label2_Click()
SOLARDATA.Show
Me.Hide

End Sub

Private Sub Label2_MouseMove(Button As Integer, Shift As Integer, X As Single, Y As Single)
Label2.ForeColor = vbWhite
```

```
End Sub

Private Sub Label3_Click()
Unload Me
End

End Sub

Private Sub Label3_MouseMove(Button As Integer, Shift As Integer, X As Single, Y As Single)
Label3.ForeColor = vbWhite

End Sub

Private Sub Label4_Click()
REPORT.Show
Me.Hide

End Sub

Private Sub Label4_MouseMove(Button As Integer, Shift As Integer, X As Single, Y As Single)
Label4.ForeColor = vbWhite

End Sub

Private Sub Label5_Click()
about.Show
Me.Hide

End Sub

Private Sub Label5_MouseMove(Button As Integer, Shift As Integer, X As Single, Y As Single)
Label5.ForeColor = vbWhite

End Sub
```




SECURITY DATA REPORT
BACK
Registrationno
Surname
FirstName
LastName
Address
City
Country
SCPOJOJO
HJKKHIHI
UGIUGIOG
YYFUGL
UUGIHIH
HJOJ;
OJOJ