**NETWORK SECRITY MODEL FOR COOPERATIVE NETWORK**

**(case study university of Jos network)**

**BY**

**DE-SHUWAL DYELKYES JAMES**

**UJ/2014/NS/0172**

**A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF NATURAL SCIENCES, UNIVERSITY OF JOS, NIGERIA IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE (B.Sc) IN COMPUTER SCIENCE**

**MARCH, 2018**

**DECLARATION**

I, DE-SHUWAL DYELKYES JAMES with the matriculation number UJ/2014/NS/0172, hereby declare that this project work was carried by me and every other external work used in this project has been duly acknowledged.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DE-SHUWAL DYELKYES JAMES Date

UJ/2014/NS/0172

**APPROVAL**

This project has been read and approved as having satisfied the requirements of the Department of Computer Science, Faculty of Natural Sciences, University of Jos, Nigeria for the award of Bachelor of Science (B.Sc) Degree in Computer Science.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dr. Godwin Thomas Date

(Supervisor)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prof. Davou N. Choji Date

(Head of Department)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prof. Afolayan Ayodele Obiniyi Date

(External Examiner)

**DEDICATION**

With gratitude in my heart, I dedicated this project work to God Almighty for his grace and mercies upon my life as a student of this great institution. I also dedicate this book to my warm, loving, and caring family.

**ACKNOLEDGEMENT**

I give thanks to God almighty for his guidance, strength and inspiration upon me throughout this project work. Thus; my deepest gratitude goes to my beloved Parent Mr. & Mrs. De-shuwal Alex A. James for their unending advice, fervent prayers and financial support in my academic pursuit, and also to our siblings for their prayers and encouragement, I say thanks to you all and I can’t stop loving you people.

I will like to also acknowledge the efforts my supervisor Dr. Godwin Thomas who even with his tight schedules, went through every bit of this work and through whose constructive criticism made the work to take its present form. Sir I render a million thanks to you sir.

I also will like to acknowledge all my course mates, set 2018 and friends who have encouraged me positively, without you this aspect of my life will not be worth remembering. Finally, I recognize all the staff of the Department of Computer Science for their encouragement and support in my academic pursuit. No man is an island and nobody is a custodian of knowledge, it is our in-depth pleasure to acknowledge all the geniuses who in one way or the other assisted in the success of this project work. God bless you all. And God bless Nigeria (Amen).

**ABSTRACT**

In recent years, as a result of the rapid development in information technology it has made computer the most preferred machine for data processing and management; thus, increasingly changed the style of living. Network security is now at the forefront of computer network related issues. With the evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly exercised attacks causing damage or committing theft.

There is a lack of reliable network security for university of Jos network; this research indicated interest in solving the problem by modelling a network security design for university of Jos network, to enhance the learning and research ability of the student and staff of the university; thus, protecting the intellectual and research properties of the institution. Thus; adhering to best practices in network security and data confidentiality. The main aim of this research is to protect the network from vulnerabilities, threats, attacks, configuration weaknesses and security policy weaknesses.

**TABLE OF CONTENTS**

[Declaration i](#_Toc508814931)

[Approval ii](#_Toc508814932)

[Dedication iii](#_Toc508814933)

[Acknoledgement iv](#_Toc508814934)

[Abstract v](#_Toc508814935)

[Table of content vi](#_Toc508814931)

[List of figures ix](#_Toc508814932)

[List of tables x](#_Toc508814933)

[Chapter 1: Introduction 1](#_Toc508812900)

[1.0 Introduction 1](#_Toc508812901)

[1.1 Background Information 1](#_Toc508812902)

[1.2 Problem Area 2](#_Toc508812903)

[1.3 Problem Statement 3](#_Toc508812904)

[1.4 Research Question 3](#_Toc508812905)

[1.5 Research Objectives 4](#_Toc508812906)

[1.6 Research Methodology 4](#_Toc508812907)

[1.7 Project Scope/Limitations 5](#_Toc508812908)

[1.8 Brief Chapter Outline 5](#_Toc508812909)

[1.8.1 Chapter 1: Introduction 5](#_Toc508812910)

[1.8.2 Chapter 2: literature review 5](#_Toc508812911)

[1.8.3 Chapter 3: proposed solution 5](#_Toc508812912)

[1.8.4 Chapter 4: design and implementation 5](#_Toc508812913)

[1.8.5 Chapter 5: Evaluation/Testing 6](#_Toc508812914)

[1.8.6 Chapter 6: Conclusion 6](#_Toc508812915)

[1.9 Conclusion 6](#_Toc508812916)

[Chapter 2: Literature Review 7](#_Toc508812917)

[2.0 Introduction 7](#_Toc508812918)

[2.1 What is network 7](#_Toc508812919)

[2.1.1 Type of network 8](#_Toc508812920)

[2.1.2 Network component 9](#_Toc508812921)

[2.1.3 network design model 10](#_Toc508812922)

[2.1.4 Characteristic of a network architectures 11](#_Toc508812925)

[2.1.5 Network Requirements 12](#_Toc508812926)

[2.2 network threats, vulnerabilities and attacks 12](#_Toc508812927)

[2.2.1 network threats 12](#_Toc508812928)

[2.3.2 Network Attacks 13](#_Toc508812929)

[2.2.3 Common network security vulnerability and attack 14](#_Toc508812930)

[2.3 Network Security solutions 17](#_Toc508812933)

[2.3.1 network security 17](#_Toc508812934)

[2.3.2 Importance of security 18](#_Toc508812935)

[2.3.3 LAN/WAN network Security 19](#_Toc508812936)

[2.3.4 Risks Assessment, Policies 20](#_Toc508812937)

[2.3.5 Network Security Model 22](#_Toc508812939)

[2.4 Characteristics of Network Security 24](#_Toc508812940)

[2.4.1 Network security architecture 24](#_Toc508812941)

[2.4.2 Why security is not a point product but a process 24](#_Toc508812942)

[2.4.3 Benefit of network security 25](#_Toc508812943)

[2.5 Conclusion 25](#_Toc508812944)

[Chapter 3: Proposed Solution 26](#_Toc508812945)

[3.0 Introduction 26](#_Toc508812946)

[3.1 Data Collection 26](#_Toc508812947)

[3.1.1 Population of the Study 27](#_Toc508812948)

[3.1.2 sampling and Instrument Design 27](#_Toc508812949)

[3.2 Findings 29](#_Toc508812950)

[3.2.1 Network Layout and Design Model 29](#_Toc508812951)

[3.2.2 Network Security Design and Policy Implementation 31](#_Toc508812954)

[3.2.3 Challenges of the Existing System 31](#_Toc508812955)

[3.3 Proposed solution 32](#_Toc508812956)

[3.4 Conclusion 33](#_Toc508812957)

[CHAPTER 4: Design and Implementation 34](#_Toc508812958)

[4.0 Introduction 34](#_Toc508812959)

[4.1 Requirement Specification 34](#_Toc508812960)

[4.1.2 Available operation: 37](#_Toc508812961)

[4.1.2 Functional Requirement 37](#_Toc508812962)

[4.1.3 Non-Functional Requirements 38](#_Toc508812963)

[2.2 System Design 38](#_Toc508812964)

[2.2.1 Network Security Policy Design Template 38](#_Toc508812965)

[2.2.2 policy design for the new system 40](#_Toc508812966)

[2.2.3 System Model 44](#_Toc508812968)

[4.3 System implementation operation 45](#_Toc508812970)

[4.4 Conclusion 51](#_Toc508812979)

[Chapter 5: Evaluation/Testing 52](#_Toc508812980)

[5.0 Introduction 52](#_Toc508812981)

[5.1 Testing 52](#_Toc508812982)

[5.2 People involved in the testing 52](#_Toc508812983)

[5.3 Test design for the model 53](#_Toc508812984)

[5.4 Conclusion 54](#_Toc508812985)

[Chapter 6: Conclusion and Future Work 55](#_Toc508812986)

[6.0 Introduction 55](#_Toc508812987)

[6.1 Brief summary of findings 55](#_Toc508812988)

[6.2 Accomplishment of objectives 56](#_Toc508812989)

[6.3 Suggestions for further research 57](#_Toc508812990)

[6.4 Conclusion 57](#_Toc508812991)

[REFERENCES 58](#_Toc508812992)

[Appendix A: dmz and router configuration 60](#_Toc508812993)

**LIST OF FIGURES**

[Fig 2.1: Hierarchical Network Design 10](#_Toc508812923)

[Fig 2.2: flat network design 11](#_Toc508812924)

[Fig 3.0: school network layout 30](#_Toc508812952)

[Fig 3.1: detailed network design of the school 31](#_Toc508812953)

[fig 4.1: new design layer out 45](#_Toc508812969)

[Fig 4.2: ping to the dns-server by admin staff, student and tech-staff 46](#_Toc508812971)

[Fig 4.4: ftp access by admin staff 47](#_Toc508812972)

[Fig 4.5.2: ssh into device by student and tech-staff from new system model 48](#_Toc508812973)

[Fig 4.6: mail transfer between users 48](#_Toc508812974)

[Fig 4.7: monitoring of traffic into dmz zone 49](#_Toc508812975)

[Fig 4.8.1: old system external resources access 50](#_Toc508812976)

[Fig 4.8.2: new system external resource access 50](#_Toc508812977)

[Fig 4.9: external user accessing unijos site 51](#_Toc508812978)

**LIST OF TABLES**

[Table: 2.0 configuration weakness 15](#_Toc508812931)

[Table: 2.1: security policies weakness 15](#_Toc508812932)

[table 2:3 risk assessment table 21](#_Toc508812938)

[Table 4.1: systems risk assessment rate level 40](#_Toc508812967)