DEVELOPMENT OF AN IMPROVED RISK ASSESSMENT MODEL IN CYBERSPACE SECURITY MANAGEMENT

BY

AKINSIKU, OMOYEMI ABIMBOLA
B.Sc. (Hons), Computer Science (Ife)

A THESIS SUBMITTED TO THE DEPARTMENT OF COMPUTER SICNECE AND ENGINEERING, FACULTY OF TECHNOLOGY,
OBAFEMI AWOLOWO UNIVERSITY, ILE-IFE

IN PARTIAL FUFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE (M.Sc.)

IN COMPUTER SCIENCE

2016

OBAFEMI AWOLOWO UNIVERSITY, ILE-IFE, NIGERIA

HEZEKIAH OLUWASANMI LIBRARY

POSTGRADUATE THESIS

AUTHORIZATION TO COPY

Author AKINSIKU Omoyemi Abimbola

Title DEVELOPMENT OF AN IMPROVED RISK ASSESSMENT MODEL IN CYBERSPACE SECURITY MANAGEMENT

Degree MASTER OF SCIENCE (M.Sc.) in Computer Science

I, AKINSIKU Omoyemi Abimbola, hereby authorize the Hezekiah Oluwasanmi Library to copy my thesis, in part or in whole, in response to request from individual researchers and / or organisations for the purpose of private study or research.

....

Signature Date

CERTIFICATION

This is to certify that this is an original research project carried out by AKINSIKU Omoyemi Abimbola with registration number TP13/14/0982 in the Department of Computer Science and Engineering, Faculty of Technology, Obafemi Awolowo University, Ile-Ife, Nigeria.

....

Prof. G. A. Aderounmu **Date**
(Supervisor)

....

Dr. (Mrs) B.O. Akinyemi **Date**
(Co-Supervisor)

....

Dr. O.A. Odejobi **Date**
(Chief Examiner)

DEDICATION

This project is dedicated to God Almighty that made it possible to start and finish the program and all those whose insistence birthed this work.

AKNOWLEDGEMENTS

A man can receive nothing, except it be given from heaven

(Holy Bible Jn 3:27)

My heart beats with mixed feelings of elation, sense of accomplishment and deep humility even as I acknowledge the grace and mercy of God in my life. Every good and every perfect gift including life and knowledge is from above, and comes down from the father of lights, with whom there is no variableness nor shadow of turning. Unto thee my Lord and God I give all praise, all honour and all glory for the completion of this study.

I received support from quite a number of people. I am particularly grateful to my supervisor, Prof. G.A Aderounmu and my co-supervisor, Dr. (Mrs) Akinyemi for their inspiring guidance, constructive criticism and valuable contributions to this study.

My darling husband, bother and friend, Olalekan and our lovely son Oluwafolajimi were very supportive and showed great understanding especially during my occasional disappearances from home.

I wish to register my profound appreciation to all staff in Computer Science , notably Dr. B.S. Afolabi, Dr. O. Oluwatope, Dr. Akhigbe, Mr. Gambo and Mrs Amoo (whose contribution during my program provided direction for the work).

My appreciation goes to my wonderful mother-in-law Mrs. Oni Omowunmi who stood by me to ensure that I had time for my research and took care of my son. I express my profound gratitude to my sweet parents who encouraged me when I was weary.

I express my gratitude to my wonderful sisters Dr. (Mrs) Aladesanmi, Mrs. Adeyemo, and Mrs. Agbotoba. Also, to my nieces Iteoluwa, Ireoluwa and Iseoluwa Aladesanmi.

I cannot but appreciate my mentor, the person who gave me the confidence to press on, Dr. Temitope Aladesanmi.

Lastly, I want to say thank you to my office colleagues , my brothers, members of the RCCG, All Sufficient One parish, and others who continue to wish me well in the inner recess of their heart. Thank you all and God bless you.

TABLE OF CONTENTS

CHAPTER TWO : LITERATURE REVIEW

CHAPTER FOUR: SIMULATION, RESULTS AND DISCUSSION

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

LIST OF FIGURES

LIST OF TABLES

LIST OF ALGORITHM

ABSTRACT

This research formulated and simulated a risk assessment model for cyberspace network security risks. This was with a view to determine the security state of the selected cyberspace network by considering the cyberspace risk concerns such as threats, attacks and vulnerabilities.

A cyberspace network was selected i.e OAUNET. The vulnerability and attack was analyzed based on the National Vulnerability Database (NVD). The ease of exploitability of the risk was determined using the Common Vulnerability Scoring System (CVSS) model. The risk assessment model was formulated using the synergy of Absorbing Markov Chain and Markov Reward Model. The graphical representation of attackers behavior was modeled using Attack Tree based on the inter-relationships between the vulnerabilities. R-Statistics Package was used to simulate the model formulated. The simulation output of the risk was presented in tables and graph.

The performance of the developed risk model was evaluated using Reliability and Availability as the evaluation measures of the model.

The simulation result shows that the expected path length of an attacker reduces as the days increases because as soon as a vulnerability is out with the exploit code it becomes easier for attackers to leverage on the exploit code to infiltrate a network. The performance of the developed model was carried out by benchmarking with an existing model. The evaluation results proved that the risk assessment of the developed model is higher in performance of reliability and the availability. The developed model was able to assess security risks of a selected cyberspace network with 86.7% reliability and *93%* availability rate, which implies, increase of 28.9% of reliability and 12% of availability respectively over the existing model. The results showed that the developed model is able to obtain a better effectiveness in optimizing the network

performances by providing information about the inherent cyberspace network risks to deliver the higher reliability and a higher availability; also, has the capability of performing long time prediction and mitigating risk occurrences.

It was concluded that the proposed assessment model measures the security risk quantitatively and predicts performances using objectives metrics and eventually improves the overall network performance efficiencies by reducing the impact or consequences of risk and being able to perform long term prediction. Thus, can be adapted for risk assessment in a network by the network administrators for more effective network management in a minimum time and at a minimum expense. This research will provide security practitioners a better understanding of the relationship between vulnerabilities and their lifecycle events and will provide information about the state of security and also remediation actions.

CHAPTER ONE
INTRODUCTION

1.1 Synopsis

Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. As Internet usage continues to expand, cyberspace will become increasingly woven into the fabric of everyday life across the globe. (National Security Strategy, 2010). Cyberspace is the collection of computing devices connected by networks in which electronic information is stored and utilized, and communication takes place. Cyberspace is in one way connected with the physical world. Cyberspace depends for its very existence on hardware, software, cables and routers. It depends on physical objects existing in physical space (Sandip, 2010).

The world is becoming more interconnected with the advent of the internet and new networking technologies. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security in cyberspace is of great importance because of intellectual property that can be easily acquired through the internet which is a unique and wholly new medium of worldwide human communication.

Cybersecurity is a whole set of procedures and systems providing protection of computer systems and networks from intentional and unintentional damages or dangers in the cyberspace through services like confidentiality, integrity, authentication, availability (Sandip, 2010). To defend a critical infrastructure is a fairly complicated task and at the same time, cybercriminals are increasingly using sophisticated social engineering techniques leading to disruptions in business operations, damaging the reputation as well as financial stability of the critical Infrastructures

(Jericho, 2014). To ensure that the overall security risk stays within acceptable limits, network practitioners need to ensure risks in the organization are measured. There has been criticism of the quantitative attempts of risk evaluation due to the lack of data for validating the methods (HyunChul and Yashwant, 2011). Security vulnerabilities that have been discovered remain unpatched for a while considering risk for an organization. Today online banking, systems, stock market trading, transportation, even universities and other higher institutions depend on the internet for computing and communications (Jacques et al., 2011).

1.1.1 University as a critical infrastructure in cyberspace

Critical infrastructure is defined as systems and assets whether physical or virtual, so vital that the incapacitation or disruption of such may have a debilitating impact on security, safety, economy, environment, or any combination of these across a federal, state, regional, territorial, or local jurisdiction (Javier *et al.*, 2012). The university is a critical Infrastructure in the cyberspace because it increasingly uses the Internet technology to communicate with other networks around the globe using the Internet Protocol (IP). The explosive growth of the Internet and its technology has related into creation of information explosion which has created a paradigm shift in knowledge creation and teaching and learning environments (Nampoori, 2010). Academia's cyber preparedness has received less media attention than that of certain retailers and financial institutions, but nonetheless the cyber risks confronting Universities are pervasive and alarming (Wylie and Jennifer, 2015). For instance, the officials at the University of Maryland reported the breaches suffered by the educational institutions at the University of Maryland on the 20th of February, 2014 where an outside source gained access to a secure records database that held information dating back to 1998, including names, social security numbers, dates of birth, and

university identification numbers for over 300,000 people affiliated with the university on two campuses (Wylie and Jennifer, 2015).

As much as universities are looking to meet the ever growing demands on computing and network performance, at the same time they need to incorporate ways of combating evolving security challenges. Perversely, this status makes the University a possible target for malicious hactivists, in addition to inadvertent cyberattacks. Thus, attempt is made in this study to analyze Obafemi Awolowo University Network (OAUNET) as a critical infrastructure in cyberspace in order to understand the security status of the network.

1.1.2 OAUNET as a network in the cyberspace

Obafemi Awolowo University is a federal university located in south-western city, ile-ife. OAUNET is a name given to the institution's campus wide computer network. OAUNET hosts the University web site and provides a web-based e-mail facility for all OAUNET registered staff, postgraduate students, undergraduate students and retired university staff. OAUNET currently connects to the internet on 400Mbps bandwidth using the gigabits network. OAUNET provides services for cooperate centers such as Centre for Energy Research and Development (CERD), National Centre for Technology Management (MACETEM), Regional Centre for Training and Aerospace Studies (RECTAS) and Obafemi Awolowo University Teaching Hospital Complex (OAUTHC) among others. The academic subnets comprising of two colleges and fourteen faculties are equipped with gigabit fibre connections serving a