

UNIVERSITI TEKNOLOGI MARA

**NETWORK SECURITY RISK ASSESSMENT BASED ON
FUZZY LOGIC APPROACH**

NURULHIDAYAH BT ABDUL LATIF

Dissertation submitted in partial fulfillment of the requirements
for the degree of

Master of Science (Information Technology)

Faculty of Computer and Mathematical Sciences

July 2012

STUDENT'S DECLARATION

I declare that the work in this report was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the result of my own work, unless otherwise indicated or acknowledged as reference work. This report has not been submitted to any other academic institution or non-academic institution for any other degree of qualification.

In the event that my report is found to violate the conditions mentioned above, I voluntarily waive the right of conferment of my degree and degree to be subjected to the disciplinary rules and regulations of Universiti Teknologi MARA.

Name of Student	Nurulhidayah Bt Abdul Latif
Student's ID No.	2010726461
Program	Master of Science (Information Technology)
Faculty	Faculty of Computer and Mathematical Sciences
Dissertation Title	Network Security Risk Assessment Based On Fuzzy Logic Approach

Signature of Student	
Date	31 st July 2012

ABSTRACT

The purposes of the study were to design a model of network security risk assessment and to assess the result from the risk assessment conducted. The threats created were dealing with the computer network which is spreading widely that might cause risk impact to the organization. Due to this condition, the security mechanism of an institution needs to determine that all the assets and information are preserving safely. Therefore, this research is focusing on risk assessment to analyze the generic threats in the education institution towards network security appliance which is called firewall. The generic threats list was chosen based on MyRAM (2005) guideline from Malaysian Administrative Modernization and Management Planning Unit (MAMPU). The qualitative method that leads to the understanding and holistic description of a phenomenon was applied in this study. This method generates rich, detail data from a multiple perspectives. The instruments used to collect data were close-ended questionnaire and interview. Questionnaire as the main source of information helped to obtain the evaluation of threats from the four experts in the network security area. In the interview session it was conducted face-to-face at the institution for a better understanding. Fuzzy Logic approach which contains Triangular Average Formula, Efficient Fuzzy Weighted Average (EFWA) and Euclidean Distance was selected as the approach in the present study. It was utilized in finding the 'Likelihood' and 'Consequence' of the threats. The result of this study revealed that firewall as the appliance was in the moderate level in which necessary measures should be taken by the particular institution to curb the threats. Risk assessment for the firewall will be conducted by using different approaches such as Bayesian, Dempster-Shafer Theory, Neural Network and Immunity Algorithm by utilizing more respondents in the future research.

ACKNOWLEDGEMENT

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

In the name of Allah the Most Gracious, Most Merciful. All praise be to Allah for giving me the endurance, patience and strength during this long, arduous journey. Only with Allah's blessings, love and help that this research has been possible.

My deepest and sincere gratitude are extended to my supervisor, Dr. Fakariah Hani Bt. Mohd Ali for her advice, insightful guidance and encouragement that she devoted in helping me to accomplish this research. I also would like to extend a special thanks to the Dissertation Coordinator of Faculty of Computer and Mathematical Sciences, Dr. Fariza Hanis Abdul Razak for her invaluable advice and assistance and also my examiner Dr. Syaripah Ruzaini Syed Aris for her advice, assistance and knowledge sharing.

My heartfelt appreciation also goes to a number of special people. My parents, Mr. Abdul Latif Bin Ibrahim and Mdm. Rohani Bt. Abdul Rahman who have encouraged me in my academic pursuit throughout my life journey and for their continuous love and prayers, my sisters especially Mdm. Noorharyati and my brothers for their support, help, patience, encouragement and endless love. My friends especially Siti Nur Iman, Wan Nur Hafizhoh, Asma, Athirah and other friends for their great help, support and encouragement. Last but not least, to Mr. Wan Mohd Nadzir Hadzril Bin Wan Ismail for his help in sharing and providing useful information about the research. This study would not have been possible with all of you. Thank you and may God bless all of you.

TABLE OF CONTENTS

	Page
STUDENT'S DECLARATION	i
ABSTRACT	ii
ACKNOWLEDGEMENT	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	viii
LIST OF FIGURES	ix
CHAPTER ONE: INTRODUCTION	
1.1 Introduction	1
1.2 Problem Statement	4
1.3 Objectives	7
1.4 Scope of the Research	8
1.5 Significance of the Research	8
1.6 Organization of the Thesis	8
CHAPTER TWO: LITERATURE REVIEW	
2.1 Overview of Network Security	10
2.1.1 Types of Network Security Threats	12
2.2 Risk Assessment	14
2.2.1 Risk Assessment Methods	18
2.2.2 Risk Assessment Process	21
2.2.3 Importance of Risk Assessment	22
2.3 Network Security Appliances	23
2.3.1 Firewall	24
2.3.2 Overview of Firewall Technologies	25