Simulation on Network Security Design Architecture for Server Room
In Rwanda Information Technology Agency

Karerangabo Eric

University of Utara Malaysia
2009
Simulation on Network Security Design Architecture for
Server Room
In Rwanda Information Technology Agency

A thesis submitted to college Arts & Sciences
in partial fulfillment of the requirement for the degree
Master of Science (Information Technology)
University of Utara Malaysia

By
Karerangabo Eric

© Karerangabo Eric, October 2009. All rights reserved
PERMISSION TO USE

In presenting this thesis in partial fulfilment of the requirements for a Master of Science in IT degree from University Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor or, in their absence by the Academic Dean College of Arts and Sciences. It is understood that any copying, publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It should also be understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean (Academic) College of Art and Sciences
University Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.
ABSTRACT

Today, computer networks attacks have continued to increase in severity and sophistication. Data lost and unavailability of network resources due to attacks from internet have negative financial impact on many companies. Unprotected organisation’s networks from internet attacks face high risk of data loss and espionage. Network devices that make up network are the most targeted in order to penetrate in companies system as some come with vulnerability from the manufacturer. In this study, network security architecture for server room had been developed for enhancing the security. Further, two simulation models had been developed to compare the throughput for both existing and developed security architecture.
I would like to express my sincere appreciation to the Almighty God, the giver of life, wisdom, knowledge and understanding. Without His grace and mercy this work would not have come to fruition.

My profound gratitude goes to my supervisor Mr. Ali Yusny bin Daud for his constructive advice, scientific proven prowess, motherly encouragement and motivation during the course of this study. Mr. Taiwo Ayankunle who taught me how to use Omnet++

This acknowledgement will not be complete without my mum, for her love and prayers, my brothers and sisters, my uncle Rukerikibaye Raphael for their financial support. My late father, the instruction you gave with love has always kept me going. I would like to conclude by appreciating all academic scholars that taught me while at UUM, other UUM staff, friends and students that made my studies easier.

KARERANGABO Eric

November 03, 2009
TABLE OF CONTENT

<table>
<thead>
<tr>
<th>PERMISSION TO USE</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>ii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>iii</td>
</tr>
<tr>
<td>TABLE OF CONTENT</td>
<td>iv</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>ix</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>x</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xi</td>
</tr>
</tbody>
</table>

CHAPTER ONE  INTRODUCTION ................................................................. 1

1.1 Background ...................................................................................... 1

1.2 Problem Statement ........................................................................... 3

1.3 Objectives ......................................................................................... 5

1.4 Scope and Limitation ........................................................................ 5

1.5 Significance of Study ....................................................................... 5

1.6 Organisation of Report .................................................................... 6

CHAPTER TWO  LITERATURE REVIEW ......................................................... 7

2.1 Network Security Overview ............................................................ 7

2.2 Issues in Network Security ............................................................. 9

2.3 Network Security Architecture ....................................................... 10
CHAPTER TWO  NETWORK SECURITY ........................................................................... 11

2.4 Network Security Model .................................................................................... 12

2.5 Simulation Model ............................................................................................... 15

2.5.1 Simulation Model Approach ....................................................................... 15

2.5.2 Simulating Computers Networks ................................................................ 16

2.5.3 Simulating Network Attacks ....................................................................... 17

2.6 Summary ............................................................................................................ 18

CHAPTER THREE  METHODOLOGY ..................................................................... 20

3.1 Network Security Development Process ............................................................ 20

3.1.1 Services Identification ................................................................................ 20

3.1.2 Asset Identification ..................................................................................... 21

3.1.3 Threat Assessment ................................................................................... 22

3.1.4 Service/Asset Relationships ..................................................................... 22

3.1.5 Risk Assessment for Assets and Services ................................................ 22

3.1.6 Policy Construction ................................................................................. 22

3.1.7 Network Security Design ........................................................................ 22

3.1.8 Implementation ....................................................................................... 23

3.1.8.1 Formulate Problem ............................................................................. 24

3.1.8.2 Objective of the Study ........................................................................ 24

3.1.8.3 Data Preparation ................................................................................. 24

3.1.8.4 Model Design ..................................................................................... 24

3.1.8.5 Coding ................................................................................................ 24
CHAPTER FOUR  DEVELOPMENT OF NETWORK  

SECURITY ARCHITECTURE

4.1  Server Room Requirements

4.1.1  Services Hosted in Sever Room

4.1.2  Skim of Existing Architecture

4.2  Security Design Consideration

4.2.1  Network Devices Identified

4.2.2  Hardening Network Devices

4.2.2.1  Hardening Switch

4.2.2.2  Hardening router

4.2.2.3  Hardening firewall

4.2.2.4  Hardening Signature-based IDS
4.2.3 Layered security protocol ................................................................. 38
  4.2.3.1 Application layer security......................................................... 38
  4.2.3.2 Transport Layer security.......................................................... 39
  4.2.3.3 Network layer security............................................................. 40
  4.2.3.4 Link Layer ............................................................................... 42
4.2.3 Identity security .................................................................................. 42

4.2.5 Segmentation and defence in depth ..................................................... 43
  4.2.5.1 Segmentation ............................................................................ 43
  4.2.5.2 Defence in depth ....................................................................... 44

4.3 Topology of security architecture ............................................................ 45

4.4 Summary ............................................................................................... 46

CHAPTER FIVE SIMULATION RESULT ....................................................... 47

5.1 Experimental design ............................................................................. 47
  5.1.1 Effect of increasing security technologies in the network on throughput .. 50

5.2 Advantage of Developed Security Design over Existing Design ................. 52
  5.2.1 Difference of both design based on security technology .................... 52

5.4 Summary ............................................................................................... 54

CHAPTER SIX CONCLUSION ................................................................. 55

6.1 Research Contribution .......................................................................... 55

6.2 Challenge and Limitation ....................................................................... 55

6.3 Recommendation and Future Work ....................................................... 56
LIST OF TABLES

Table 5.1: The Initial Parameters and Symbols of existing design simulation model ................................................................. 49

Table 5.2: The Initial Parameters and Symbols of new design simulation model .... 49

Table 5.3: Throughput of existing and new design ................................................................. 51

Table 5.4: Security technologies for both security architectures ................................. 52

Table 5.5: attacks detected by those security technologies ........................................ 53
LIST OF FIGURES

Figure 2.1: Spam attacks by continent (Sophos, 2009)......................................................... 9

Figure 3.1: Network security development process (Yang et al., 2006)......................... 21

Figure 3.2: Flow Diagram of the methodology (Law et al., 2001)......................... 23

Figure 3.3: Hierarchy of Modules in OMNeT++ (Vargas, 2005)........................... 27

Figure 4.2: Network security Architecture................................................................. 45

Figure 5.1: The Simulation model.............................................................................. 48
LIST OF ABREVIATIONS

RITA: Rwanda Information Technology Agency
DMZ: Demilitarized Zone
ICT: Information communication technology
LAN: Local Area Network
FTP: File Transfer Protocol
HTTP: Hypertext Transfer Protocol
DNS: Domain Name Service
DoS: Denial of Service
IDS: Intrusion Detection System
IPS: Intrusion Protection System
AAA: Authentication, Authorization and Accounting
CA: Certificate Authority
OSI: Organisation Standard
VPN: Virtual Private Network
VLAN: Virtual Local Area Network
ACL: Access List
TCP/IP: Transmission Communication Protocol/ Internet Protocol
UDP: User Datagram Protocol
DHCP: Dynamic Host Configuration Protocol
CHAPTER ONE

INTRODUCTION

This chapter presents the aim of this project. Background, problem statement and objectives are discussed. Therefore, project scope and the benefit of the project are highlighted as well organization of report.

1.1 Background

Rwanda Information Technology Agency (RITA) is a high powered Think-Tank with the mission to lead the process of creating the Rwanda information society and developing the economy in line with the aspirations of the vision for Rwanda. The Agency’s responsibility is to advice the Government on all matters relating to how best Rwanda can formulate, develop and implement its ICT policies, strategies and plans to speed up the process of transforming Rwanda into an information-rich, knowledge-based society and thereafter its economy.

RITA aims at consolidating and coordinates the country’s information technology resources in order to realize the larger road-map of the country for the future. RITA coordinates the implementation of the government strategic resource and at the same time, attempts to manage the national ICT procurement and delivery process to ensure that the Government gets value for financial investment, by using ICT to support the delivery of e-Government services to all its citizens.
The contents of the thesis is for internal user only
REFERENCE


\textit{A Framework for Teaching Network Security Courses.}


Wei S., Mirkovic J. & Swany M., 2005. Distributed worm simulation with a realistic Internet model. PADS.