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

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.

ACKNOWLEDGEMENTS

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

PERMISSION TO USE i

ABSTRACT ii

ACKNOWLEDGEMENTS iii

TABLE OF CONTENT iv

LIST OF TABLES ix

LIST OF FIGURES x

LIST OF ABREVIATIONS xi

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

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

3.1.8.6 Validate the Model 25
3.1.8.7 Running of Experiments 25
3.1.8.8 Analysis of the Simulation 25
3.1.8.9 Documentation 25
3.1.9 Audit and Improvement 26
3.2 Modelling in Omnet++ 26
3.2.1 Omnet Modules Connection 27
3.2.2 Omnet++ Model Components 29
3.3. Summary 29
CHAPTER FOUR DEVELOPMENT OF NETWORK .....
SECURITY ARCHITECTURE 30
4.1 Server Room Requirements 30
4.1.1 Services Hosted in Sever Room. 30
4.1.2 Skim of Existing Architecture 30
4.2 Security Design Consideration 31
4.2.1 Network Devices Identified 32
4.2.2 Hardening Network Devices 32
4.2.2.1 Hardening Switch 33
4.2.2.2 Hardening router 34
4.2.2.3 Hardening firewall 37
4.2.2.4 Hardening Signature-based IDS 37

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

REFERENCE 57

APPENDIX A: RESEARCH SCHEDULE (GANTT CHART) 62

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

Amer H. and Hamilton A., 2008. Understanding Security Architecture. *Proceeding of SpringSim conference. Auburn University Auburn, Alabama 36849-5347, USA.*

Ashley M. ,2006. Layered Network Security: a best practice approach. White paper. StillSecure.

Backfield J. 2008. Network Security Model. SANS Institute Reading room, retrieved from: www.sans.org/info/36909

Bai Y., Summers W., & Bosworth E., 2007. Teaching Network Risk Assessment to Online Graduate Students. *Information Security Curriculum Development Conference '07, September 28-29, 2007, Kennesaw, Georgia, USA.*

Bhatt D. V.,Schulze S., & Hancke G. P., 2006. Secure Internet Access to Gateway Using Secure Socket Layer. IEEE transactions on instrumentation and measurement, vol. 55, no. 3, june 2006

Bouchard M., 2009. The Next Step in Network Security for Enterprises. White paper.

Broda M**.** Nortel's Network Security Architecture: New dimensions in network security.

Brown S. G. & Yip F., 2006. Integrating Pattern Concepts & Network Security Architecture. IEEE journal

Bye, R., Schmidt S., Luter K., & Albayrak, 2008. Application-level simulation for network security. *Proceeding of Simulation tools March 03 - 07, 2008, Marseille, France.*

Chen J., Wang X. & He L., 2008. An Architecture for Differentiated Security Service. *Proceeding of International Symposium on Electronic Commerce and Security, DOI*

10.1109/ISECS.2008.65

Convery S., 2004. *Network Security Architectures. Expert guidance on designing secure networks.* Cisco Press.

Deal R. A., 2005. Cisco Router Firewall Security. *Harden perimeter routers with Cisco Firewallfunctionality and features to ensure network security*. Cisco Press. 800 East 96th Street. Indianapolis, IN 46240 USA.

Deccio T. C, 2004. Network-Layer Selective Security. Master thesis.

F5 Networks, Inc, 2006. Unified Access and Application Delivery Methodology. White Paper.

Idika N. C., Marshall B. H. & Bhargava B. K., 2009. Maximizing Network Security Given a Limited Budget. In proceeding at *Tapia'09,* April 1-4, 2009, Portland, Oregon, USA.

Hilley S., 2002. Network security architecture without perimeters. Journal *Incorporating E- Commerce, Internet and Telecommunications Security*

Kartalopoulos S. V., 2008. Differentiating Data Security and Network Security. IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

Kettani M. & Debbagh T., 2008. NCSec – A National Cyber Security Referential for the Development of Code of Practice in National Cyber Security Management. In proceeding of ICEGOV2008, December 1-4, 2008, Cairo, Egypt.

Kuhl M. E., Sudit M., Kistner K., & Costantini K., 2007. Cyber attack modeling and simulation for network security analysis. *Proceedings of the 2007 Winter Simulation*

Conference

Martinez D., 2008. Protecting Critical Infrastructure: Implementing Integration and Expanding Education. *SIGCAS Computers and Society, Volume 38, No. 1, March 2008.*

Law & McComas (2001). How to build valid and credible simulation models. *Procedings of the 2001 Winter simulation Conference.*

Liska A., 2003. The Practice of Network Security. Deployment Strategies for Production Environments. Prentice Hall PTR.

Lammle et al, 2005. CCSP. *Complete Study Guide (642-501, 642-511, 642-521, 642-531, 642-541*. Cisco press.

Lincke S. J. & Holland A., 2007. Network Security: Focus on Security, Skills, and Stability. 37th ASEE/IEEE Frontiers in Education Conference October 10 – 13, 2007, Milwaukee, WI

Liljenstam M., Liu J., Nicol D., Yuan Y., Yan G., and Grier C., 2005. Rinse: The real-Time immersive network simulation environment for network security exercises. *Proceedings of the Workshop on Principles of Advanced and Distributed Simulation (PADS'05).*

Mallery J. & Kelly P., 2005. Hardening network security. Scisco press.

Mohamad R.,2004. Network Security Architecture. *Proceedings of South Central Conference, JCSC 19, 4.*

Neumann PG, 2000. Practical Architecture for Survivable System and Networks. SRI International, retrieved from : http://www.csl.sri.com/users/neumann/survivability.pdf

Peng C., Zhang Q., & Tang C., 2009. Improved TLS Handshake Protocols Using

Identitybased Cryptography. 2009 International Symposium on Information Engineering and Electronic Commerce. 2009 IEEE

Porras P. & Shmatikov V., 2006. LargeScale Collection and Sanitization of Network Security Data: Risks and Challenges. *Proceeding at NSPW 2006, Schloss Dagstuhl, Germany*.

Rahman S., Nguyen T. A., & Yang T. A., 2006. Developing certificate-based projects for web Security classes. Mid-south conference.

Riley F., 2003. The Georgia Tech Network Simulator. *In Proceedings of the ACM SIGCOMM workshop on Models, methods and tools for reproducible network research.*

Rufi A., 2007. Network security. 1 and 2 companion guide. . Cisco Press.

Stawowski M., 2007. The Principles of Network Security Design. *Nortel Technical Journal,Issue 3, ISSA Journal.*

Schmidt M., Smith M., Fallenbeck N., Picht H. & Freisleben B., 2007. Building a Demilitarized Zone with Data Encryption for Grid Environments. *GridNets 2007*, October 17–19, 2007, Lyon, France. .

Schudel G., 2007. Router Security Strategies: Securing IP Network Traffic Planes. Cisco Press.

Shieh, A., Myers, A. C., and Sirer, E. G. 2008. A stateless approach to connection-oriented protocols. *ACM Transactions on Computer Systems, Vol. 26, No. 3, Article 8, Publication date: September 2008.*

Tidwell T., Larson R., Fitch K., and Hale J., 2001. Modeling Internet Attacks. Proceedings of the 2001 IEEE. Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001

Yang T. A. & Nguyen T. A., 2006. Network Security Development Process. *A Framework for Teaching Network Security Courses.*

Watkin A & Wallace K., 2008. CCNA Security. Official Exam Certification Guide. Cisco Press.

Kaeo M., 2004. Designing Network Security. A practical guide to create a secure network infrastructure. Second Edition. Cisco Press.

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