# NETWORK SECURITY MANAGEMENT AUDIT AT UUM COMPUTER CENTRE

A thesis submitted to the Faculty of Information Technology in partial fulfillment of the requirements for the degree
Master of Science (Information Technology)
Universiti Utara Malaysia

by

Mohamad Fadli Bin Zolkipli

**JABATAN HAL EHWAL AKADEMIK**
**(*Department of Academic Affairs*)**
**Universiti Utara Malaysia**

**PERAKUAN KERJA KERTAS PROJEK**
***(Certificate of Project Paper)***

Saya, yang bertandatangan, memperakukan bahawa
*(I, the undersigned, certify that)*

**MOHAMAD FADLI BIN ZOLKIPLI**

calon untuk Ijazah
*(candidate for the degree of )* **MSc. (IT)**

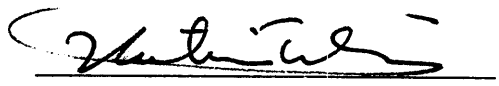
telah mengemukakan kertas projek yang bertajuk
*(has presented his/ her project paper of the following title)*

**NETWORK SECURITY MANAGEMENT AUDIT AT UUM COMPUTER CENTRE**

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
*(as it appears on the title page and front cover of project paper)*

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
*(that the project paper acceptable in form and content, and that a satisfactory knowledge of the filed is covered by the project paper).*

Nama Penyelia Utama
*(Name of Main Supervisor)*: **ASSOC. PROF. HATIM MOHAMAD TAHIR**

Tandatangan
*(Signature)* : 

Tarikh
*(Date)* : 21/6/04

# PERMISSION OF USE

In presenting this thesis in partial fulfillment of the requirements for a post-graduate degree from Universiti 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 purposes may be granted by my supervisor(s) or, in their absence, by the Dean of the Faculty of Information Technology. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti 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 of Faculty of Information Technology**
**Universiti Utara Malaysia**
**06010 UUM Sintok**
**Kedah Darul Aman**

# ABSTRAK

Organisasi hendaklah menilai keselamatan rangkaian meraka bagi mengenalpasti 'accountability', 'confidentiality', 'integrity', 'authority' dan juga 'authenticity'. Kaedah yang biasanya digunakan bagi tujuan ini adalah dengan menjalankan audit. Dengan menggunakan kaedah pengauditan, kajian ini cuba untuk menilai keselamatan rangkaian di Pusat Komputer UUM. Tujuan kertas kerja ini dibuat adalah untuk mengenalpasti ketidakcekapan di dalam pengurusan keselamatan rangkaian di Pusat Komputer UUM. Hasil keputusan dari pengauditan keselamatan rangkaian ini akan digunakan untuk mencadangkan penyelesaian bagi meningkatkan ketidakcekapan yang dialami. Kaedah pengauditan yang telah dipilih adalah daripada Information Protection and Security Division of University Computing Services (IP & SD UCS), dari The State University of New Jersey.

# ABSTRACT

An organization needs to evaluate its network security in order to measure the accountability, confidentiality, integrity, authority and also its authenticity. The method that is commonly used for this purpose is by conducting an audit. Using the auditing method, this research attempts to evaluate the network security at the UUM Computer Centre. The purpose of this paper is to identify the network security deficiencies at UUM Computer Centre. Results from the network security audit will then be used to recommend solution to improve those loopholes. The selected audit method is based on the Information Protection and Security Division of University Computing Services (IP & SD UCS), from The State University of New Jersey.

# ACKNOWLEDGEMENTS

I wish to acknowledge my gratitude to the Universiti Utara Malaysia, Sintok, Kedah Darul Aman for providing the facilities for this research undertaking. The same goes to my family and the members of master students, which since the inception of this study has given me their full support.

I wish to acknowledge the support of the supervisors, namely Assoc. Prof. Hatim Mohamad Tahir whose labored endlessly supervise me in time, all the way to its final reproduction.

This study would not have materialized without the cooperation and support from the UUM Computer Centre. I wish to thank all staff at UUM Computer Centre for providing the documents and assist on the audit fieldwork. The contributions to the success of this study are very much appreciated.

Finally, I pray with most thankful to Allah SWT for being most gracious in blessing this study. Without His blessing, this study would not have been possible.

Mohamad Fadli Bin Zolkipli
June, 2004

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

The change in computer network and telecommunication including Internet technology and wireless networking now has enable organization and people to communicate more quickly and extensively. It has made the business or management activities more effective, easier and faster. However, one of the criteria that can not be avoided is the security aspect in order to measure the trust of computer network and information. Basically, proper and effective network security provides the following criteria:

- Accountability - proof that an intended transaction indeed took place.
- Confidentiality - protection of confidential information from an eavesdropper.
- Integrity - assurance that the information sent is the same as the information received.
- Authority - assurance that those who request data or information are authorized to do so.
- Authenticity - assurance that each party is who they say they are.

Security is a significant consideration in Local Area Network (LAN), especially in the organizational network that connected to the Internet for local or remote access. Cisco System (2001) defined Internet as a "term used to refer to the largest global internetwork, connecting hundreds of thousands of networks worldwide using the TCP/IP protocol stack". The Internet is not owned or controlled by any single entity or organizations.

The contents of the thesis is for internal user only

# REFERENCES


Baltatu, M. Lioy, A. Maino, F & Mazzocchi, D. (2000). Security issues in control, management and routing protocols. *Computer network.* Vol. 34. pp. 881-894.

BICSI (2001). *Chapter 8 Network Security; Network Design Reference Manual.* 4th Edition.

Cisco System (2001). *A Beginner's Guide to Network Security.* United States of America; Cisco Press. Retrieved August 24, 2003, from http://www.pcconnection.com

Desrosiers, M. (2003). Security Analysis and Audit. *A.P. Lawrence Home.* Retrieved March 20, 2004, from http://www.aplawrence.com/MDesrosiers/securityaudit.html

Federal Information Processing Standards (1994). Specifications for Guideline for The Analysis Local Area Network Security. *Federal Information Processing Standards Publication 191.*

Frank, J. G. & Joel, G. S. (2001). Security Issues on the Internet. *The CPA Journal.* Retrieved March 20, 2004, from http://www.nysscpa.org/cpajournal/2001/1000/dept/d106401.htm

Hayes, B. (2003). Conducting a Security Audit: An Introductory Overview. *SecurityFocus.* Retrieved April 22, 2004, from http://www.frame4.com/php/modules.php?name=News&file=article&sid=514

Leinwand, A. & Conroy, K. F. (1996). Network Management; A Practical Perspective. 2nd Edition. Canada; Addison Wesley Longman, Inc. pp. 76.

Michael, D. (2003). Security Analysis and Audit. *A.P. Lawrence Home.* Retrieved April 22, 2004, from http://www.aplawrence.com/MDesrosiers/securityaudit.html

National State Auditors Association and the U. S. General Accounting Office (2001). *Management Planning Guide for Information Systems Security Auditing.* Retrieved April 22, 2004, from http://www.gao.gov/special.pubs/mgmtpln.pdf

Oppenheimer, P. (2001). *Top-Down Network Design.* United States of America; Cisco Press. pp. 250-251.

Rutgers, The State University of New Jersey (2004). *Risk Assessment.* Retrieved April 22, 2004, from http://rusecure.rutgers.edu/sec_plan/risk.php

Sam, M. (2001). *Logical Security of the City's Local Area Network.* Audit Report. Retrieved March 20, 2004, from http://talgov.com/citytlh/auditing/index.html

Slade, R. (2002). Glossary of Communications, Computer, Data, and Information Security Terms. Version 0.09. Retrieved April 22, 2004, from http://victoria.tc.ca/int-grps/books/techrev/secgloss.htm

Stopa K. B. (2003). A Network Security Audit Methodology. *GIAC Security Essentials Certification (GSEC).* Practical Version 1.4, Option 1. Retrieved March 20, 2004, from http://www.giac.org/practical/GSEC/Kim_Stopa_GSEC.pdf

Sullivan, K. Kelley, K & McElveen, M. (2001). Network Audit Procedures. *CVOC Technology Library Project.* Retrieved March 20, 2004, from http://isds.bus.lsu.edu/cvoc/Projects/TechLibrary/NetAudit/Alternative%20Comparison.htm

Tanenbaun, A. S. (1996). *Computer network.* United States of America; Prentice Hall.