PRELIMINARY ANALYSIS OF INTRUDER DETECTION SYSTEM IN UUM

A thesis submitted to the Graduate School
in partial fulfilment of the requirements for the degree
Master of Science (Information Technology), Universiti Utara Malaysia.

by

Ibrahim bin Yusof

Sekolah Siswazah
(Graduate School)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certification of Project Paper)

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

IBRAHIM B. YUSOF

calon untuk Ijazah
(candidate for the degree of) Sarjana Sains (Teknologi Maklumat)

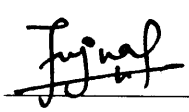
telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

PRELIMINARY ANALYSIS OF INSTRUDER DETECTION SYSTEM IN UUM

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 field is covered by the project paper).

Nama Penyelia
(Name of Supervisor) : Prof. Madya Dr. Zurinah Suradi

Tandatangan
(Signature) : 

Tarikh
(Date) : 25/03/02

PERMISSION TO USE

In presenting this thesis in partial fulfilment of the requirements for a postgraduate 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 supervisors or, in their absence, by the Dean of the Graduate School. 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 Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

ABSTRAK

Era teknologi maklumat membuatkan kita amat bergantung kepada perkhidmatan yang diberikan oleh sistem dan rangkaian komputer. Namun begitu kebanyakan sistem maklumat berkomputer yang digunakan di dalam kehidupan seharian menyediakan amat sedikit perlindungan terhadap manipulasi dan penyalahgunaan sistem komputer tersebut. Kajian awal ini menyediakan laporan yang menjurus kepada isu-isu teknikal asas yang berkaitan dengan pencerobohan komputer dan pengkelasannya.

Objektif kajian ini adalah untuk menganalisa dan memahami perlakuan asas aktiviti pencerobohan komputer dan menilai pandangan pengguna mengenai keselamatan komputer serta keperluan pemasangan sistem pengesan pencerobohan.

Analisa adalah berasaskan data yang dikutip dari soal selidik yang dijalankan di dalam organisasi. Dalam proses penyelidikan ini, pengkelasan secara sistematik telah dijalankan terhadap data mengenai aktiviti pencerobohan sebagai kaedah menganalisa data. Ciri-ciri pengkelasan utama termasuklah penceroboh, objektif penceroboh, alat yang digunakan, cara capaian dan hasil dari pencerobohan.

Hasil dari kajian ini termasuklah pengkelasan terhadap pencerobohan dan dapatan baru mengenai gelagat penceroboh yang dipanggil serangan dalaman yang amat merbahaya tetapi merupakan ancaman keselamatan yang selalu diabaikan. Kajian ini juga menjelaskan pandangan pengguna berkenaan perlaksanaan sistem keselamatan di dalam organisasi serta keperluan sistem pengesan pencerobohan.

ABSTRACT

There is a rapidly increasing dependence on services provided by these computer systems and networks but most computerized information systems we use in our everyday lives provide very little protection against hostile manipulation. This preliminary study presents report focused on the fundamental technical issues of computer intrusion and their taxonomy.

The objective of this study is to analyze and understand the nature of intrusion activity and perception of the user regarding the security policy and the implementation of intrusion detection system in the organization.

The analysis is based mainly on the data from questionnaires given to the staff in the organization. Throughout this work, systematic categorization of data that related to intrusion has been used as the main method for data analysis. The main categorization of intrusion includes the intruder, their objective, tools used, access method and result of intrusion.

The results of this work include the taxonomy of the intrusion and new findings about the behavior of so-called insider attackers; a dangerous but sometimes neglected security threat. It also explores the perception of the user regarding security implementations and requirement of intrusion detection system in the organization.

ACKNOWLDGEMENT

Along the way, I have received help and support from many persons and party, to whom I would now like to express my sincere gratitude. The first person I thank is my supervisor, Assoc. Prof. Dr. Zurinah Suradi. Her wise guidance and dedicated support has been of immense value to me. Assoc. Prof. Dr. Zurinah great sense of humor and understanding makes it fun to work with her.

Next, I thank the other members of M.Sc. (IT) student (in order of appearance): Mohd Zukime, Shamsuri Abdullah, Che Abdul Rani, Cikgu Hashim and Cikgu Azizan. We have had some times of hard work together, but also great fun when we have prepared our papers. It has been a privilege to work with you all.

I also thank other past and present staff and academicians at the Universiti Utara Malaysia for their dedicated efforts in education and research and for contributing to a friendly learning atmosphere especially to Prof. Abu Talib Othman, Assoc. Prof. Dr. Wan Rozaini, Assoc. Prof. Nazib Nordin, Assoc. Prof. Ku Ruhana, Assoc. Prof. Shahrum Hashim, En Hilmi Hussein, En. Shakirin Shaari, En Mohd Suki, Puan Huda and the late En Zamberi Saat.

Last, but not least, I dedicate this work to my family. It would not have been possible to combine my two roles as a father and a Master student without the rock solid support from my beloved wife Marizan Che Ramli that making my dreams come true. To my children, Amalina and Mohd Fithri, thank you for all the happiness you give us.

Finally, I thank my parents Yusof bin Ulah and Fatimah bte Sahak, not only for breeding and feeding me, but for letting me grow.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Advances in computer and communication technologies have resulted in highly integrated distributed systems that allow users to access information and resources from all over the globe. With many access points, computer system can easily be hacked or attacked. Rapid increase in the number of reported intrusions, break-ins and computer thefts results in an ever-increasing need for applying effective computer security measures such as firewall system, intrusion detection system and better security policy.

Despite the undeniable progress made in network and computer security over the past few years, network devices and computers are still vulnerable from inside attack as well as outside attack. Today, when more and more of the valuable assets of an organization are in the form of information stored in computerized information systems, the security of the systems has become a critical issue.

However, little attention was given to security issues in the design of most systems that are in use today. As a matter of fact, people who should have

The contents of the thesis is for internal user only

REFERENCES

Amoroso, E (1999). *"Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response"*. Intrusion.Net Books, Sparta, New Jersey.

Anderson, J.P. (1980). "*Computer security threat monitoring and surveillance*". Technical report, James P Anderson Co., Box 42, Fort Washington, PA 19034, USA, April 15,

Anderson, T.E. (1993). "Management guidelines for PC security", *Proceedings of the 1992 ACM/SIGAPP Symposium on Applied Computing (Vol. II): Technological Challenges of the 1990s*, Kansas City, KS.

Angel, I. (1993). "Computer security in these uncertain times: the need for a new approach", *Proceedings of the 10th International Conference on Computer Security, Audit and Control (CompSec)*, London, October.

Attanasio, C. R, Markstein. P. W, and Philips, R. J, (1976). "Penetrating an operating system: a study of VM/370 integrity". *IBM Systems Journal*, 15(1):102–116.

Bishop, M., Cheung, S. and Wee, C. (1997). "The threat from the net [Internet security]", *IEEE Spectrum*, Vol. 34 pp. 8.

Brian Tung (1999). "*The Common Intrusion Detection Framework* (CIDF)". http://gost.isi.edu/cidf/.-12/01/2001

British Standards Institution (1995). "*Code of Practice for Information Security Management*", BS 7799.

Cohen, F.B. (1995). "Protection and Security on the Information Superhighway", *John Wiley & Sons*, New York.

Davis, F. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, September, pp. 319-40.

Denning D. E. and Neumann P. G. (1985). "Requirements and model for IDES—a real-time intrusion detection expert system". Technical report, *Computer Science Laboratory, SRI International, Menlo Park*, CA 94025-

3493, USA.

Garfinkel and Spafford, (1996). *"Practical UNIX and Internet Security: Second Edition"*, O'Reilly & Associates, Inc.

Goodhue, D.L. and Straub, D.W. (1989). "Security concerns of system users: a proposed study of user perceptions of the adequacy of security measures", *Proceedings of the 21st Hawaii International Conference on System Science (HICSS), Kona, HA.*

Harrington, S.J. (1996). "The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions", *MIS Quarterly*, Vol. 20 pp. 33-41,

Helman, P. and Liepins, G (1993). "Statistical foundations of audit trail analysis for the detection of computer misuse". *IEEE Transactions on Software Engineering*, 19(9):pp.886–901.

Howard J. D. (1997). *"An Analysis of Security Incidents On The Internet 1989– 1995". PhD thesis*, Carnegie Mellon University, Pittsburgh, Pennsylvania.

Icove, D., Seger, K and VonStorch, W. (1995). *"Computer Crime: A Crimefighter's Handbook"*, O'Reilly & Associates, Inc., Sebastopol, CA.

Jonsson E. (1998). "An integrated framework for security and dependability". *In Proceedings of the New Security Paradigms Workshop*, pages 22–29, Charlottsville, Virginia, September 22–25. ACM Press, New York.

Jonsson E. and Olovsson T. (1997). "A quantitative model of the security intrusion process based on attacker behavior". *IEEE Transactions on Software Engineering*, 23(4):235–245.

Jonsson, E. (1995). *"A Quantitative Approach to Computer Security from a Dependability Perspective". PhD thesis*, School of Electrical and Computer Engineering, Chalmers University of Technology, Goteborg, Sweden.

Jonsson, E. (1998). "An integrated framework for security and dependability". *In Proceedings of the New Security Paradigms Workshop, pages 22–29*, Charlottsville, Virginia. ACM Press, New York.

Ko C. (1996). *"Execution Monitoring of Security-Critical Programs in a Distributed System: A Specification-Based Approach"*. PhD thesis, University of California at Davis.

Kowalski, S. (1990). "Computer ethics and computer abuse: a longitudinal

study of Swedish university students", *IFIP TC11 6th International Conference on Information Systems Security*.

Krsul I. V. (1998). "*Software Vulnerability Analysis*". PhD thesis, Purdue University, West Lafayette, Indiana.

Kumar S. (1995). "*Classification and Detection of Computer Intrusions*". PhD thesis, Purdue University, West Lafayette, Indiana.

Lackey R.D. (1974). "Penetration of computer systems an overview". *Honeywell Computer Journal*, 8(2):81–85.

Laprie, J.C. (1992). "Dependability: Basic Concepts and Terminology of Dependable Computing and Fault-Tolerant Systems. Springer-Verlag, Vienna. Volume 5.

Linde, R (1975). "Operating system penetration". *In Proceedings of the National Computer Conference, volume 44 of AFIPS Conference Proceedings*, pages 361–368, Anaheim, California, May 19–22,1975. AFIPS Press, Mont-vale, New Jersey.

Lindqvist, *et. al.,*(1997). "How to systematically classify computer security intrusions". *Proceedings of the 1997 IEEE Symposium on Security & Privacy*, pages 154–163, Oakland, California, USA. IEEE Computer Society Press.

Mounji A. (1997). "Languages and Tools for Rule-Based Distributed Intrusion Detection". *PhD thesis,* Institut d'Informatique, University of Namur, Belgium.

Neumann, P. G. (1978). "Computer system security evaluation". *In Proceedings of the National Computer Conference, volume 47 of AFIPS Conference Proceedings*, pages 1087–1095, Anaheim, California, June 5–8, 1978. AFIPS Press, Montvale, New Jersey.

Neumann, P.G. (1995). "*Computer-Related Risks*". ACM Press and Addison-Wesley, New York.

Neumann, P.G. (1999). "*Practical architectures for survivable systems and networks: Phase-one final report*". Technical report, Computer Science Laboratory, SRI International, Menlo Park, CA, USA.

Nie, N.H. and Erbring, L (2000). "*Internet and society a preliminary report*". Stanford Institute for The Quantitative Study Of Society.

Olovsson T. (1995). "*Practical Experimentation as a Tool for Vulnerability*

Analysis and Security Evaluation". PhD thesis, School of Electrical and Computer Engineering, Chalmers University of Technology, Goteborg, Sweden.

Powler N. (2000). "*Everything You Need to Know About Intrusion Detection."* www.axien.com-22/10/2001.

Rushby, J. (1994). "Critical system properties: Survey and taxonomy". *Technical Report CSL-93-01, Computer Science Laboratory,* SRI International, Menlo Park, CA 94025-3493.

Russell, D. and Gangemi, G. T. S. (1991). "*Computer Security Basics"*, O'Reilly & Associates, Inc., Sebastopol, CA.

Saltzer, J.H, and Schroeder, M.D. (1975). "The protection of information in computer systems". *Proceedings of the IEEE*, 63(9):1278–1308.

Sebring M, Shellhouse E, Hanna M. E, and Whitehurst R. A. (1988). "Expert systems in intrusion detection: A case study". *In Proceedings of the 11th National Computer Security Conference*, pages 74–81, Baltimore, Maryland, October 17–20, 1988.

Smaha S. E. (1988). "Haystack: An intrusion detection system". *In Proceedings of the Fourth Aerospace Computer Security Applications Conference*, pages 37–44, Orlando, Florida, December 12–16, 1988. IEEE Computer Society Press, Los Alamitos, California.

Vaccaro H. S. and Liepins G. E. (1989). "Detection of anomalous computer session activity". *In Proceedings of the 1989 IEEE Symposium on Security and Privacy*, pages 280–289, Oakland, California. IEEE Computer Society Press, Los Alamitos, California.