INTELLIGENT AGENTS IN MANAGING A CENTRALIZED ANTI-VIRUS SOLUTION

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

By
Jazlina binti Ahmad Azahari

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)

JAZLINA BINTI AHMAD AZAHARI

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

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

INTELLIGENT AGENTS IN MANAGING A CENTRALIZED ANTI-VIRUS SOLUTION

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 MOHAMED TAHIR**

Tandatangan
(Signature) :

Tarikh
(Date) : 26/2/05

PERMISSION TO USE

In presenting this thesis in partial fulfillment 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 purpose may be granted by my supervisor(s) 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

Agen ditakrifkan terbaik sebagai perisian yang berkeupayaan menyelesaikan masalah tanpa memerlukan sokongan dan tanpa melibatkan kawalan pengguna. Agen-agen yang bekecerdasan seharusnya berupaya menyesuaikan diri mereka terhadap persekitaran, berupaya mempelajari, rasional dan berkomunikasi antara satu sama lain. Perisian bernama *Trend Virus Control System* (TVCS) yang dihasilkan oleh syarikat Trend Micro telah dikenalpasti dan dipilih sebagai model yang mencontohi agen pintar. Analisa *Strengths Weaknesses Opportunities* dan *Threats* (SWOT) serta rangka kerja *Five Domains Security Model*, digunakan di dalam mengkaji perisian TVCS. Diagram *Fish Bone* pula digunakan untuk memberi gambaran keseluruhan tentang riskio-risiko keselamatan rangkaian bank yang dikaji. Kajian ini mengemukakan dua penyataan cadangan, pertama, TVCS menggunakan pendekatan yang digunakan oleh agen pintar, kedua, agen TVCS mendedahkan risiko-risiko keselamatan terhadap rangkaian Bank XYZ. Akhir sekali, saranan-saranan turut dibuat berdasarkan pengenalpastian terhadap risiko-risiko keselamatan tersebut untuk memperkukuhkan tahap keselamatan rangkaian Bank XYZ. Walau bagaimanapun, masih tiada jawapan yang muktamat dan yang benar-benar sah untuk menyokong pernyataan-pernyataan cadangan yang dikemukakan di dalam kajian ini. Oleh kerana itu, kajian-kajian susulan sepatutnya dibuat oleh penyelidik-penyelidik untuk meneruskan penerokaan di dalam bidang ini.

ABSTRACT

Agents are best defined as software with the ability to solve problems independently without any intervention or assistance from the user. Agents with intelligence characters would be able to adapt themselves to environment, be able to learn, rationalize and also communicate to with one another. A software named Trend Virus Control System (TVCS) produced by Trend Micro, has been identified and selected as a model to emulate as an intelligent agent. The Five Domains of Security Model is used as a framework to analyze the security aspects of the bank's network. The study uses Strengths Weaknesses Opportunities and Threats (SWOT) analysis to examine TVCS. A Fish Bone diagram is also illustrated to give an overview of the security risks posed by intelligent agents. The study offers two propositions. Firstly, TVCS uses an intelligent agent approach. Secondly, TVCS agents pose security risks to Bank XYZ network. Finally, recommendations are made based on identification of the security risks to strengthen level of security of Bank XYZ network. However, in this study, there are still no definite and confirmed answers to the stated propositions. Therefore, follow-up studies should be made by other researchers to further investigate the area.

ACKNOWLEDGMENTS

First of foremost, I would like to thank God for the courage, strength and patience that you gave me.

I also wish to thank the following people who have contributed directly, indirectly and sometimes unknowingly to the completion of this project.

A huge appreciation to my supervisor, Associate Professor Hatim Mohd Tahir, the core person in making this a reality, my husband, Azly, who has always been there for me during sunny or rainy days, my 1-year-old son, Amirul Amnan who is unknowingly, behaves as a good son, and all the cooperative people (you know who you are) in getting me there.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BIOS	–	Basic Input/Output System
CAGR	–	Compound Annual Growth Rate
CGI	–	Common Gateway Interface
CIO	–	Chief Information Officer
DMZ	–	DeMilitarized Zone
DNS	–	Domain Name System
FBI	–	Federal Bureau Investigation
FWE	–	External Firewall
FWI	–	Internal firewall
HTTP	–	HyperText Transfer Protocol
ICSA	–	International Computer Security Association
IDC	–	International Data Corporation
IETF	–	Internet Engineering Task Force
IIS	–	Internet Information Service
IMSS	–	Internet Messaging Security Suite
IP	–	Internet Protocol
IPSec	–	Internet Protocol Security
ISO	–	International Standards Organization
ISP	–	Internet Service Provider
ISVW	–	InterScan Virus Wall
IT	–	Information technology
LAN	–	Local Area Network
LDAP	–	Light Weight Directory Access Protocol
MAS	–	Multi-Agent System
OLE	–	Object Linking Embedding
OS	–	Operating system
OSI	–	Open System Interconnection
RADIUS	–	Remote Authentication Dial-In User Service
SMTP	–	Simple Mail Transfer Protocol

SSD	–	Systems Security Department
SWOT	–	Strengths Weaknesses Opportunities Threats
TVCS	–	Trend Virus Control System
URL	–	Uniform Resource Locator
VB	–	Visual Basic
WWW	–	World Wide Web

1. INTRODUCTION

Computer security is an important issue. Attacks on computer systems and networks are on the rise and the sophistication of these attacks continues to escalate to alarming levels. The proliferation of personal computers, local area networks (LAN) and distributed processing has drastically changed the way we manage and control information resources (Louw & Duffy, 1992; Gottschalk, 1995; Geiger, 2000). Experts estimated that the true cost of computer crime amounts to billions of dollar annually. This amount includes costs associated with clean-up, loss of data, liability, and lost of customer confidence. These losses show how security is important to all aspects of information technology including intelligent agents.

Intelligent agents are very active research topic these days. Agents are smart due to programming codes that tell them actions, ways to do them and time to do them (Muller, 1997). According to Franklin and Graesser (1996), agents differ from programs because output from agents would normally affect what they sense later. An agent need not be a program at all but software agents are, by definition, programs, but a program must match up to several marks to be an agent. They also classified agents according to their characters. For example, mobile agents are intelligent agents that are able to transport themselves from one machine to another. During the migration process the information associated with mobile agents moves with them. This enables a mobile agent to gather information on different computers and learn in real time, as it progresses. Multi-agent systems (MAS) is another type of intelligent agent, in which there are a number of agents, having specific roles within some system or organization, and being capable of interacting with each other and with their environment.

The contents of the thesis is for internal user only

REFERENCES

Allport, W. (1961). *Patterns in growth and personality*. New York: Holt, Rinehart and Winston.

Austrainer. (1999). *Developing your strategic SWOT analysis*. This is not a paper. Retrieved July 7, from the World Wide Web: http://www.austrainer.com/archieves/1397.htm

Bakry, S. (2003). Development of security policies for private network. *Journal of Network Management*, 13, 203-210.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, 25(4).

Bhagyavati, H., & Hicks, G. (2003). A basic security plan for a generic organization. *Journal of Computing Sciences in Colleges*, 19(1).

Bernstein, T., Bhimani, A., Schultz, E., & Siegel, C. (1996). *Internet security for business*, Wiley: Computer Publishing.

Bloombecker, B. (1990). Spectacular computer crimes: What they are and how they cost American business half a billion dollars a year. Illinois: Dow-Jone Irwin, Homewooe.

Bonatti, A., Krauss, S., Salinas, J. & Subrahmanian. (1998). Data–security in heterogeneous agent systems. *Cooperative Information Agents*, 290-305.

Brustoloni, J. (1991). Autonomous Agents: Characterization and Requirements, *Carnegie Mellon Technical Report CMU-CS-91-204*, Pittsburgh: Carnegie Mellon University.

Butler, G. (1997). *Securing the enterprise network*. South Carolina: Computer Technology Research Corporation.

Cause and Effect Diagram. This is not a paper. Retrieved November 5, 2001 from the World Wide Web: http://www.dartmouth.edu/~ocer/CQI/Ishikawa.html

Coordination Center (2003). http://www.cert.org.

Charles, V. (1997). Boston Sortware Newspaper, 1997 Edition. *Raptor Systems: Putting teeth in security*. This is not a paper. Retrieved July 13, 2003 from the World Wide Web: 2003.http://www.charlesvermette.com/raptor.html

Chess, D. (1998). Security issues in mobile code systems. *Mobile Agents and Security*, 1-14.

Cohen, F. (1987). Computer viruses-theory & experiments. *Computers and Security*, 6(6): 22-35.

Cusumano, M. (2004). Who is liable for bugs and security flaws in software?. *Communications of the ACM*, 47(3), 25-27.

Davydov, M. (2000). EIP: The Second Wave. *Information Supply Chain, 3*(4).

Durfee, H., & Lesser, R. (1988). Predictability versus Responsiveness: Coordinating problem solvers in dynamic domains. *In Proc. Of the 7th National Conf. On Artificial Intelligence*, 66-71.

Eisenhardt, K. (1989). Building theories from case study research. *Academy of Management Review*, 14, 532-50.

ESJ. (1999). 20% of Companies lack IT security policies, standards. *Enterprise System* Journal, 14(11): 12.

Faltings, B. (2000). Intelligent Agents: software technology for the new millennium. *Intelligent Agents*. Informatik.

Fites, P., Johnston, P., & Kartz, M. (1989). *The computer virus crisis*. New York : Van Nostrand Reinhold.

Flint, J. (2000). Authenticating VPN with radius. *Network Computing*. This is not a paper. Retrieved July 7, from the World Wide Web: http://www.networkcomputing.com/1114/1114ws1.html

Franklin, S., & Graesser, A. (1996). Is it an agent or just a program? Taxonomy for autonomous agent. *Intelligent Agents III*, 21-35, Berlin.

Geiger, R. (2000). *Back to information security basic*. This is not a paper. Retrieved July 7, from the World Wide Web: http://www.info-defense.com

Giorgini, P., Kolp, M., & Mylopoulos, J. (2002). Multi-Agent architectures as organizational structures. *Mobile and Network Applications*. Kluwer Publishing.

Gondek, R., Rollie,G., & Strassberg, K. (2002). *Firewalls: The Complete Reference*. New York: McGrawhill-Osborne Media.

Gordon, D. (2000). APT Agents: Agents that are adaptive, predictable, and timely. *In Proc. Of the 1st Goddard Workshop on Formal Approaches to Agent-based systems, FAABS'00*.

Gottschalk, P. (1995). *Technology Management* (in Norwegian: Teknologiledelse), Norway: Fagbokforlaget, Bergen.

Hafner, K., & Markoff, J. (1991). *Cyberpunk outlaws and hackers on the computer frontier*. New York: Simon and Schuster.

Harrington, T. (1999). Safe under the security blanket. *Computing*, 3 June, 37-40.

He, Q. & Sycara, K. (1998). *Towards a secure agent society. In Proc. Of the Workshop on Deception, Fraud and Trust in Agent Societies*, ACM.

Hoffer, A., George, F. & Valacich, S. (1996). *Modern System Analysis and Design*. California: The Benjamin/Cummings Publishing Company, Inc.

Hruska, J. (1990). *Computer Viruses and Anti Virus Warfare*. New York: Ellis Horwood,

Internet Security Software Market Forecast and Analysis, 2000 -2004, 13 July 2003. This is not a paper. Retrieved July 7, from the World Wide Web:
http:// www.idc.com

ISO/ IEC TR 12382: *Information Processing Vocabulary*; International Standards Organization, Geneva, Switzerland.

Jastia, A. (2003). Setting up a more secure network: A case study. *The Information and Communications Technology Journal*, Fujitsu, 2(2), 7-10.

Kaminka, G. & Tambe, M. (2000). Robust Agent Teams via Socially-Attentive Monitoring. *Journal of Artificial Intelligence Research* 12, 105-147.

Kendall, J. & Kendall, A. (1999). Information Deleivery Systems: An exploration of web pull and push technologies. *Communications of the AIS*, 1(14).

Kendall, J. , and Kendall, E. (1999) "Web pull and push technologies: The emergence and future of information delivery systems," in K. E. Kendall (ed.) *Emerging Information Technologies: Improving Decisions, Cooperation, and Infrastructure*, Thousand Oaks, CA: SAGE Publications, Inc.

Kirn, S., & Petsch, M. (2001). Intelligent software agents: Security issues of a new technology. *Intelligent Software Agents*. Idea Group Publishing.

Konstan, A., Miller, M., Maltz, D., Herlocker, L., Le, R., & Ridle, J. (1997) GroupLens: Applying collaborative filtering to Usenet

News, *Communications of the ACM*, March, 3(40), 77-87.

Yang Kun, Guo Xin & Liu Dayou, (2000). Security in mobile agent system: Problems and approaches. *National Natural Science Fund and 863 high-tech project*. Changchun: Department of Computer Science, JiLin University.

Landreth, B. (1989). Out of the inner circle: The true story of a computer intruder capable of cracking the nation's most secure computer systems. Tempus, Redmond, Wash.

Levin, B. (1990). *The Computer Virus Handbook*. CA: Osborne McGraw-Hill.

Louw, E. & Duffy, N. (1992). *Managing computer viruses*. New York: Oxford University Press.

Minsky, M. (1985). The Society of mind, New York: Simon and Schuster.

Mark de Rijk. (2003). *Case study: Implementing Trend Micro anti-virus solutions in the enterprise*. SANS Institute. This is not a paper. Retrieved July 7, from the World Wide Web: http://www.sans.org/rr/antivirus.php

Marx, A. (2002). *One Virus engine is not enough*. GFI Software. Germany. This is not a paper. Retrieved July 7, from the World Wide Web: http://www.gfi.com/

Marx, A. (2002). *The case for maximizing network protection with multiple anti-virus scanners*.This is not a paper. Retrieved July 7, from the World Wide Web: http://www.gfi.com/

Meeker.M, DePuy, C. (1996).*Morgan Stanly US Investment Research*. 13 July 2003. This is not a paper. Retrieved July 7, from the World Wide Web: http://a1408.g.akamai.net/7/1408/770/81e14c46464532/www.morganstanley.com/institutional/techresearch/pdfs/inet05.pdf, 13/7/03

Minolli, D. (1991). *Telecommunications Technology Handbook*, Artech House.

MoonNet: *A list of publicly traded Internet related companies (12 October, 1996)*. This is not a paper. Retrieved July 13, from the World Wide Web: http://www.moonnet.com/net/index.html

Muller, N. (1997). Improving network operations with intelligent agents.

International Journal of Network Management, (7): 116-126.

Nitin Acharekar (2003). *The Business of Security.* Computer World. Vol. 13 Issue No. 8, 1 June - 10 July 2003.This is not a paper. Retrieved July 7, from the World Wide Web: http://computerworld.com.my/pcwmy.nsf/unidlookup/115929EA E1145FA148256D3C000F2992?OpenDocument

NCC. *Telecommunications Management: Network Security.* The National Computing Center Limited. (1992).

Nwana, S., Lee, L., & Jennings, R. (1996). Co-ordination in Software Agent Systems. *BT Technol J*, 14(4), 79-88.

Omicini, A., Zambonelli, F., Klusch, M. & Tolksdorf, R. (2001). *Coordination of Internet Agents. Springer Verlag.*

Parker, D. (1976). *Crime by computer.* New York: Chas Scribeners Sonds.

Pereira, B. (2003) *Enterprise Security: Chinks in the armor.* This is not a paper. Retrieved July 13, 2003 from the World Wide Web: http://www.networkmagazineindia.com/200112/cover1.htm -

Ploskina, B. (1999). *Centralised anti-virus management is becoming critical (Industry Trend or Event).*

Porter, M. (1980). *Competitive strategy: Techniques for analysing industries and competitors.* New York: Free Press.

Reback, A., Smith, I. (1996) *Remote access security: An overview.* This is not a paper. Retrieved July 12 July, 2003. from the World Wide Web: http://www.securitytechnet.com/resource/rsc-center/vendor-wp/shiva/security.pdf

Rosenchein, S., & Zlotkin, G. (1994). *Rules of encounter: Designing conventions for automated negotiation among computers.* The MIT Press.

Smart messaging via agents, rules & filters. *Network Computing.* (2003). This is not a paper. Retrieved October 6, from the World Wide Web: http://www.networkcomputing.com/822/822ws1.html

Stoll, C. (1989). *The cuckoo's egg tracking a spy through the maze of computer episionage.* New York: Doubleday.

SWOT Analysis, Strengths, Weaknesses, Opportunities, Threats." *PMI-Plus, Minus, Interesting. 1999.* This is not a paper. Retrieved July 7, from the World Wide Web: http://www.mindtools.com/swot.html

BHC (1999). *Swoting your way to success*. This is not a paper. Retrieved July 7, from the World Wide Web: http://www.bradhuckleco.com.au/swot.htm.

Tambe, M. (1997). Towards flexible teamwork. *Journal of Artificial Intelligence Research, 7,* 83-124.

Undercoffer, J., Perich, F., Cedilnik, A., Kagal, L. & Joshi, A. (2003). A secure infrastructure for service discovery and access in pervasive computing. *Mobile Networks and Applications 8*, 113-125.