ACTIVE FIREWALL MECHANISM AS A COMPREHENSIVE APPROACH TOWARDS MINIMIZING INTERNET THREATS

CAHYO CRYSDIAN

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

MARCH 2006

ACKNOWLEDGEMENTS

First of all, I would like to thank and express my deepest gratitude and appreciation to my supervisor, Professor Dr. Abdul Hanan bin Abdullah, for his patience, advice, continuous support, and guidance. I also would like to thank to the individuals who indirectly contribute to this thesis, among them are Assoc. Prof. Dr. Mohd. Noor bin Md. Sap for inspiring me with the research works, and Professor A. H. Christer from University of Salford for valuable suggestions and constructive feedback. My appreciations are also addressed to the Research Management Center, the School of Graduate Studies, and the Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia for opening the opportunity to conduct a research study.

It has been an enjoyable discussions and interactions with my fellow university colleagues, among them are Amrifan, Heri, Tutuk, Sony, Hendriyawan, Nazori, Haris, Anis Saggaf, Agung, Lalu, Deni, Muladi, Rival, Fikri, Hudha, Marwan, Nasir, Dr. Agus Setyobudi, Dr. Asri Ngadi, Yazid, Dr. Perwira Mulia, Mbak Jati, Dahliyus, Satria, Faisal Zafar, Witcha and Siriporn, Reza and Badrisham, Azah Kamilah, Maznah, Bu Wita and Pak Kamil, Kak Ina, Kak Shidah, Kak Lijah, Kak Hasnah, Kak Lili, and many more. And my thanks to Dr. Dwi Tjahyanto to introduce me to Malaysia.

Finally, my grateful thanks, esteem, and all other admiration to my parents, Enggarsyah and Supartini, my brother, Amal Ashardian and his family, my sisters Dian Dahlia Dhamayanti and her family, and Etta Erinda Enggarini, my wife Ariana Listuhayu Wahyuni, my daughter Citra Dewi Cassimira Cahyanti, and my family in law for giving me the real love, pray, and all they have, and to support me in times of ups and downs.

ABSTRACT

Network firewalls have been receiving a lot of critics from the Internet community since many security incidents originated from the Internet could successfully bypass firewall protection. This condition is caused by the incapability of firewalls to cope with the rapid growth of the Internet technology, especially for dealing with active content. The static behaviour of the firewall becomes the root of this problem. Motivated by this condition, this study aims to improve the security of network firewalls by activating its mechanism. Here, active firewall is defined as a firewall aware of the conditions of its surrounding network and capable to identify and to develop the security requirements for guarding the protected network. To implement the active firewall, a security strategy to combat the Internet threats is defined by developing an Internet access model that consists of the models of intranet users and external parties. Three security strategies were formulated, i.e. minimizing unprotected internal users, minimizing untrusted external parties, and minimizing the interaction between unprotected internal users and untrusted external parties. Hence, the implementations of active firewall that consist of initialisation and runtime processes follow these strategies. In the initialisation process, three methods were developed namely close-condition, open-condition and lattice-based. In the runtime process, three methods were also developed, namely fuzzy-based, agent-based, and zero-based configuration. The combinations between each initialisation and each runtime process produced five active firewall systems, namely *OF*, *LF*, *OA*, *LA*, and *CZ*. Evaluations on each active firewall system were based on RFC 2979, a standard behaviour of and requirements for Internet firewalls. Two stages of evaluations were conducted, namely security analysis and comparative study. The results of the evaluations showed that active firewall was capable to combat Internet threats. And it was also proven that *LA* delivers the best security and usability compared to other proposed active firewall methods.

ABSTRAK

Sistem dinding api rangkaian komputer menerima banyak kritikan dari pengguna sejak pelbagai ancaman keselamatan dapat melepasi sistem pertahanannya. Keadaan ini disebabkan oleh perkembangan keupayaan teknologi dinding api tidak selari dengan perkembangan teknologi rangkaian yang berkembang dengan pesatnya, terutamanya yang berkaitan dengan kandungan Internet yang aktif**.** Ciri statik yang ada pada dinding api dikatakan sebagai punca kepada masalah di dalam sistem keselamatan rangkaian ini. Oleh yang demikian, kajian ini bertujuan memperbaiki tahap keselamatan dinding api rangkaian, dengan mengaktifkan mekanismanya. Dinding api aktif didefinasikan sebagai dinding api yang sensitif terhadap perubahan yang berlaku di dalam persekitaran rangkaian. Ia juga berkeupayaan mengenalpasti serta membina keperluan bagi keselamatan pertahanan rangkaian. Bagi melaksanakan model ini, strategi keselamatan terhadap ancaman Internet dikenalpasti dengan membina model capaian Internet yang mengandungi model pengguna intranet dan pihak luaran. Tiga kaedah dibentuk dalam strategi ini iaitu menggurangkan pengguna dalaman yang tidak dikawal, menggurangkan pihak luaran yang tidak dipercayai, dan mengurangkan interaksi antara pihak dalaman dan pihak luaran. Seterusnya, proses inisialisasi dan proses masa larian dalam dinding api aktif dilaksanakan mengikut strategi yang ditetapkan. Bagi proses inisialisasi, tiga kaedah dibangunkan iaitu keadaan-tertutup, keadaan-terbuka dan kaedah berasaskan kekisi. Sementara bagi proses masa larian pula, kaedah berasaskan fuzzy, kaedah berasaskan agen dan konfigurasi berasaskan sifar dibina. Gabungan bagi kedua-dua proses ini menghasilkan lima sistem dinding api aktif iaitu *OF*, *LF*, *OA*, *LA* dan *CZ*. Seterusnya, penilaian ke atas setiap sistem tersebut dibuat berdasarkan kepada sistem penilaian piawai tindakbalas keperluan sistem dinding api Internet, iaitu RFC 2979. Pada peringkat penilaian ini, dua fasa dilakukan iaitu analisa keselamatan dan kajian perbandingan. Keputusan penilaian menunjukkan dinding api aktif yang diperkenalkan mampu untuk bertahan dari ancaman Internet. Seterusnya, ia terbukti bahawa LA menghasilkan sistem keselamatan yang lebih kukuh dan kebolehgunaan yang lebih baik berbanding kaedah lain yang dibina.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

C,c	-	canals
f(a)	-	function of *a*
i,j	-	integer numbers
lc(a)	-	location of *a*
m	-	index of external parties
n	-	index of internal user
nm(a)	-	name of *a*
p	-	protection index
P(a)	-	probability of *a*
ref	-	reference
rp(a)	-	running process of *a*
S	-	safety factor
sz(a)	-	size of *a*
t	-	time
th(a)	-	threat of *a*
up	-	unprotection index
v	-	speed
x	-	index of experiment
$\forall a$	-	all *a*
$\exists a$	-	there exist *a*
$\wedge$	-	and
$\vee$	-	or
Δt	-	time duration
μ_a	-	fuzzy membership function of *a*
υ	-	mean average

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Nowadays Internet becomes more and more important to many organisations due to the advantages delivered by the Internet to support and facilitate their business and activities. The needs for Internet access exist on broad and different activities. They range from doing a simple and daily routine such as updating antivirus database, reading stock market index, and obtaining weather report, to a complex and critical task such as conducting e-commerce and bank transaction. In fact, to some organisations Internet has become their main tool to conduct the business. Besides its benefit, Internet is widely known to become the sources of many security incidents as well (Anagnostaskis *et al.*, 2003; Huang *et al.*, 2004; Lai, 2004). Therefore organisations having Internet connection needs to give more protection to their information system and internal network in order to reduce or even to eliminate the Internet threat. Commonly this strategy is implemented by installing firewall between the protected internal network or intranet and the outside network or Internet.

During the first decade of its discovery i.e. in 1980 to 1990, firewalls had gained so much popularity (Arbaugh, 2002). However, the effectiveness of firewall to enforce security has been called into question recently. In the last three years, there are dozens reports disclosing the security incidents happening in many business and private information systems originated from and even facilitated by Internet.

Consider the following facts. In September 2002, Bugbear Internet virus was first spotted in Malaysia, and within 24 hours this virus was spreading in over 100 countries and infecting million computers (Cherry, 2002). In October 2003, Spammers were reported for stealing the customers email addresses from Orbitz, the online travel agency (Associated Press, 2003). In June 2004, mysterious Internet virus stealing credit card information designed by a group of Russians was detected spreading through hundreds or possibly thousands of infected websites (Wired, 2004; Pruitt, 2004). In October 2004, Purdue's computer system was cracked by hackers that successfully gained unauthorized access to its internal network (Associated Press, 2004). This attack forced users to change their password. The security incidents above show that current firewall technology exhibit serious vulnerabilities that can easily be exploited to commit attacks. In this thesis, this issue is addressed in order to afford better intranet protection.

1.2 Background of Study

The mechanism of firewall to establish intranet protection has been receiving a lot of critics recently. Indeed, some reports disclosed the vulnerabilities of current firewall implementations. Arbaugh (2002; 2003) described the flaws of firewall as being insensitive when it deals with the active content of Internet such as ActiveX and Javascript, user mobility, and peer-to-peer technology. While Eschelbeck (2000) and Hunt and Verwoerd (2003) highlighted the security problems of firewall caused by it's static behaviour. The static character of firewall shows that current firewall implementations depend heavily on the configuration and security rules explicitly defined by network administrator. This configuration is created at start-up and maintained along the duration of the firewall, without considering the condition of the surrounding network. Thus it is not surprising that many firewall implementations cannot cope with the raising threats of Internet.

Meanwhile CERT surveys on the threat of Internet showed that during the year 2002, 2003, and 2004, malicious code in terms of worms and automatic intrusion become the most serious threats endangering many organization networks

(CERT, 2002; CERT, 2003; CERT, 2004). These results are similar to the survey conducted by Whitman (2003) and CSI/FBI Annual Computer Crime and Security Survey (Power, 2002) that produced deliberate software attacks and virus, respectively as the top rank of Internet threat. In fact, the report of Zetter (2004) supported the above survey results. It disclosed that 45% of executable files downloaded from Internet such as Kazaa contain malicious code in term of viruses, worms, and Trojan horses.

Confronting the above survey results with the critics on firewall security discloses a fact that technological improvements of Internet contents have been undermining the intranet protection provided by current firewall technology. Although this phenomenon can be easily discovered from many organization networks, however survey held by CERT on electronic crimes (CERT, 2004) showed that firewall are still considered as the most effective security tools for protecting the trusted intranet from the danger of Internet. The survey also showed that firewall becomes the most common security technology deployed to combat electronic crimes. Therefore it is crucial to upgrade the mechanism of firewall in order to enable firewall to cope with the raising threats of Internet.

Some research groups notably have been developing smart firewall mechanisms, with the purpose to enable firewall aware of the security condition of surrounding network. The work of Eschelbeck (2000) in Network Associates to develop active security initiated the development of this field by introducing active firewall system i.e. firewall collaborate with other security tool, such as IDS and anti virus, in order to recognize any intrusion and possible vulnerabilities of protected network. This approach however drew some critics from the researchers, such as Kamara *et al.* (2003) who reported the appearance of denial of service in Gauntlet active firewall, the product of implementing this method. Moreover, Haixin *et al.* (2000) emphasized a number of possible security issues might be driven by the firewall such as the problem of asymmetric routing and the decrease of performance.

Referring to the surveys of Internet security that highlighted malicious code as the most serious threat (CERT, 2002; Power, 2002), Arbaugh (2002) applieds a different approach to provide intranet protection. In this work, he developed an

active security management after learning the incidents of Code Red worm, which the spreading of this code could not be prevented although the software patch for stopping it's spreading and it's action had been available. This method puts greater responsibility on the management of the organization to manage network security manually. However, by considering the rapid growth of malicious code that increases from year to year (Kientzle and Elder, 2003), this approach would probably create more burdens to the management and fall short in the implementation.

Considering the importance of the firewall to many organization networks, and learning from the past lessons for providing more secure systems, a well-defined security strategy that appropriately combats the Internet threat while at the same time facilitating the connection to external parties is required. Thus, a study on activating the mechanisms of network firewall would become a promising approach in dealing with this issue.

1.3 Objectives

As discussed in the research background, the reason for conducting this study is due to the incapability of existing firewall methods to deal with the threat from the Internet driven by the growth of the Internet technology. The static behaviour of firewall is highlighted to cause this problem. In fact, based on CERT survey (CERT, 2004) firewalls are still required by most organization information systems to establish internal network protection. Thus, the main objective of this study is to develop appropriate strategy for protecting intranet from the threats of Internet. The methods to activate and to improve the mechanism of firewall are observed. The expectation is to have an approach capable to recognize any possible threats originating from Internet, and to restrict the Internet threats from entering the protected intranet. To accomplish this task, the study needs to achieve the secondary objectives as follows:

(i) Formulating the security strategy to combat the Internet threats. This strategy is built by identifying the possible security conditions caused from accessing Internet.

(ii) Developing a model of active firewall to host the implementation of the security strategy developed in point (i).

(iii) Formulating and developing active firewall methods in the implementation of each security strategy developed in point (i) in order to combat the Internet threats.

(iv) Conducting evaluation on each active firewall method in order to measure the applicability of network firewall to provide intranet protection. Security analysis on each method together with comparative study among the developed methods and to known firewall techniques are held in this study

1.4 Research Scopes

To conduct properly this study, the conditions limiting the research are set up as follows:

(i) It is assumed that network packets passing through the firewall are not encrypted. Or if the packets are encrypted, then it is assumed that they can be decrypted easily. This assumption greatly reduces the effort to deal with the content of the packets, thus the work can be focused on observing the mechanism to activate the firewall.

(ii) It is assumed that the speed to transfer data from the Internet to the intranet or vice versa is faster than the speed required by the internal user to communicate with more than one external party, or jumping from one external party to the other. Thus, at any time the internal user would only be able to communicate with an external party.

(iii) With regard to the mechanisms of network firewall, the security methods developed in this study are intended to guard the gate of intranet. Thus, any mechanism to secure the individual host, user, and application residing inside the intranet, are not taken into account since this operation required a mechanism that is beyond the capability of network firewall.

1.5 Outline of Research Methodology

In this study, the methodology for conducting research can be outlined as the following steps:

(i) Identifying the sources of Internet threats. This step is done by developing a model of Internet access, thus any condition causing the present of Internet threats can be recognised. To develop an Internet access model, a model of internal users and a model of external parties are built, in which set theory is used to formulate each model. Since Internet access is merely the interaction between internal users and external parties, hence intersecting both last models produces the model of Internet access.

(ii) Developing the security to combat the Internet threats. Following the identification of security conditions causing the Internet threats as formulated in step (i), a set of security strategies is defined to deter the Internet threats. It is achieved by minimizing any conditions that contribute to the threats.

(iii) Developing a model of active firewall to enable the implementation of security strategy defined in step (ii). The concept of canalisation is employed in developing this model. It is worth to note that steps (i) to (iii) are presented and discussed in Chapter 3.

(iv) Formulating and implementing the mechanism of active firewall to implement the security strategies defined in step (ii). This step consists of

two main implementation stages, namely the initialisation and runtime process of active firewall. The former is described in Chapter 4, while the latter in Chapters 5 to 7. In this stage, Redhat Linux operating system is used to develop the mechanism of firewall. It is due to the work of Patton *et al.* (2000) that proves the capability of firewall developed under Linux operating system consistently having higher transaction throughput compared to some commercial firewall such as Cisco firewall.

(v) Evaluating the developed active firewall methods. Evaluations are conducted in two stages. The first stage is to measure the usability of each method to serve Internet transaction by analysing some network parameters such as processing time, sensitivity, and accuracy. Different methods would be tested using different parameters since each method has its own operational domain. It is necessary to note that step (iv) and the first stage of evaluation are discussed in Chapters 5 to 7. Meanwhile, the second stage of evaluation as described in Chapter 8, consists of two sub-stages namely security analysis and comparative study. Security analysis is conducted based on RFC 2979, the standard behaviour of and requirements for Internet firewall. The comparative study is to compare the developed active firewall systems with the existing firewall methods i.e. no firewall, static, and dynamic firewall configuration. Upon completing this stage, the ranking of active firewall methods in term of security and usability could be determined, thus the best approach for activating network firewall can be known.

1.6 Organisation of the Thesis

This thesis is organised as follows. Chapter 1 describes the background, objective, scope, and the outline of research methodology of the study. Chapter 2 presents the results of studying the literatures in the effort of developing firewall technology. Chapter 3 discusses the concept of active firewall and formulating the strategy to combat Internet threats. A generic model of intranet users, a generic model of external parties, a model of Internet access, and active firewall model are also presented in this chapter. Chapter 4 presents the development of the initialisation process of active firewall, and the development of the runtime process is presented in Chapters 5 to 7. Chapter 5 specifically deals with the adaptive update of security rules using fuzzy-logic reasoning in which the content of network packet originating from external parties are evaluated. Chapter 6 describes a mechanism to monitor the activities of internal users by scrutinizing the running process of each internal host using distributed agent-based module. And Chapter 7 introduces zero-based configuration to minimize the available services at runtime. Chapter 8 conducts the evaluation on all of the methods proposed above using security analysis and comparative study with the known firewall methods. Finally, the conclusion, contributions, and future works of this study are given in Chapter 9.

REFERENCES

Alexander, D.S., Anagnostaskis, K.G., Arbaugh, W.A., Keromytis, A.D. and Smith, M.S. (1999). *The Price of Safety in an Active Network.* Journal of Communications and Networks (JCN), special issue on Programmable Switches and Routers. March 2001. 3(1): 4-18.

Anagnostaskis, K.G., Greenwald, M.B., Ionnidis, S., Keromytis, A.D., and Li, D. (2003). *A Cooperative Immunization System for an Untrusting Internet.* 2003. 11th IEEE International Conference on Networks (ICON). September/October 2003. Sydney, Australia: IEEE, 403-408.

Anthony, R.N. (2003). *Management Accounting: A Personal History*. Journal of Management Accounting Research. ABI/INFORM Global.15: 249-253.

Arbaugh, W.A. (2002). *Active Systems Management: The Evolution of Firewalls*. Invited paper to the 3rd International Workshop on Information Security Applications. August 2002. Cheju Island, Korea, 19-30.

Arbaugh, W.A. (2003). *Firewalls: An Outdated Defense*. In IEEE Computer. June 2003. 36(6): 112-113.

Associated Press. (2003). *Spammers Steal E-mail Address from Orbitz*. Weekly Magazine InformationWeek. 29 October 2003. http://www.informationweek.com

Associated Press. (2004a). *Hackers Crack Purdue's Computer System*. CNN Technology. 22 October 2004. http://www.cnn.com

Associated Press. (2004b). *CoolWebSearch A Spyware Mystery: Who's Behind it?*. CNN Technology. 2 November 2004. http://www.cnn.com

Bellovin, S.M. (1999). *Distributed Firewalls*. In ;login, The USENIX Magazine. November 1999. 37-39.

Bernades, M.C. and Moreira, E.D.S. (2000). *Implementation of an Intrusion Detection System Based on Mobile Agents*. International Symposium on Software engineering for Parallel and Distributed Systems. June 2000. Limerick, Ireland: IEEE, 158-164.

Castano, S., Fugini, M., Martella, G., and Samarati, P. (1995). *Database Security*. Great Britain: ACM (Association for Computing Machinery) Inc Press.

CERT. (2002). *CERT Coordination Center 2002 Annual Report*. CERT Coordination Center Annual Report. http://www.cert.org

CERT. (2003). CERT *Coordination Center 2003 Annual Report*. CERT Coordination Center Annual Report. http://www.cert.org

CERT. (2004). *2004 E-Crime Watch Survey™: Summary of Findings*. CERT Coordination Center. http://www.cert.org

Cherry, S.M. (2002). *All the Ills that Flesh is Heir To: Internet Viruses Can Get Worse-Much Worse*. IEEE Spectrum. November 2002. IEEE, 52.

Christodorescu, M., and Jha, S. (2003). *Static Analysis of Executable to Detect Malicious Patterns*. In 12th USENIX Security Symposium. August 2003. Washington DC, USA: USENIX, 169-186.

Davies, R.M. (2002). *Firewalls, Intrusion Detection Systems and Vulnerability Assessment: A Superior Conjunction?*. Network Security. 2002(9): 8-11.

Denning, D.E. (1976). *A Lattice Model of Secure Information Flow*. Communications of ACM, 1976. 19(5): 236-243.

Eschelbeck, G. (2000). *Active Security: A Proactive Approach for Computer Security Systems*. Journal of Network and Computer Applications. April 2000. 23(2): 109-130.

Freed, N. (2000). *RFC 2979 – Behavior and Requirements for Internet Firewalls*. Internet RFC/STD/FYI/BCP Archives. October 2000. Network Working Group, Request for Comments: 2979.

Garkinfel, S., and Spafford, G. (1997). *Web Security and Commerce.* USA: O'Reilly and Associates.

Goncalves, M. (2000). *Firewalls: A Complete Guide*. USA: McGraw Hill Osborne Media.

Green, S., Hurst, L., Nangle, B., Cunningham, P., Somers, F., and Evans, R. (1997). *Software Agents: A Review*. A Trinity College Dublin: Technical Report.

Guan, J., Liu, D.X. and Wang, T. (2004). *Applications of Fuzzy Data Mining Methods for Intrusion Detection Systems.* ICCSA 2004, Lecturer Notes on Computer Science 3035. Springer 2004: 706-714.

Haixin, D., Jianping, W., and Xing, L. (2000). *Policy-Based Access Control Framework for Large Networks*. Proceedings of IEEE International Conference on Network (ICON 2000). 5-8 September 2000. Singapore: IEEE, 267-272.

He, M., and Leung, H. (2002). *Agents in E-Commerce: State of the Art.* Knowledge and Information Systems. July 2002. 4(3): 257-282.

Hernandez, J.C., Sierra, J.M. and Ramos, B. (2001). *Search Engines as a Security Threat*. IEEE Computer. October 2001. 34(10): 25-30.

Hickman, B., Newman, D., Tadjudin, S., Martin, T. (2003). RFC 3511 - Benchmarking Methodology for Firewall Performance. Internet RFC/STD/FYI/BCP Archives. April 2003. Network Working Group, Request for Comments: 3511.

Hicks, M., Keromytis, A.D. and Smith, J.M. (2003). *A Secure PLAN*. IEEE Transactions on System, Man, and Cybernetics-Part C: Applications and Review, August 2003. 33(3): 413-426.

Huang, Y.W., Yu, F., Hang, C., Tsai, C.H., Lee, D.T., and Kuo, S.Y. (2004). *Securing Web Application Code by Static Analysis and Runtime Protection.* World Wide Web 2004. May 17-22, 2004. New York, USA: ACM, 40-51.

Hunt, R., and Verwoerd, T. (2003). *Reactive Firewalls: A New Technique*. Elsevier Journal on Computer Communications. July 2003. 26(12): 1302-1317.

Hwang, K. and Gangadharan, M. (2001). *Micro-Firewalls for Dynamic Network Security with Distributed Intrusion Detection*. IEEE International Symposium on Network Computing and Applications. October 2001.Cambridge, MA, USA: IEEE, 68-79.

Ioannidis, S., Keromytis, D., Bellovin, S.M., and Smith, J.M. (2000). *Implementing a Distributed Firewall.* 7th ACM Conference on Computer and Communication Security. 1-4 November 2000.Athens, Greece.

Kamara, S., Fahmy, S., Schultz, E., Kreschbaum, F., and Frantzen, M. (2003). *Analysis of Vulnerabilities in Internet Firewalls*. Elsevier Computer and Security 2003. 22(3): 214-232.

Kayssi, A., Harik, L., Ferzli, R. and Fawaz, M. (2000). *FPGA-Based Internet Protocol Firewall Chip*. The 7th IEEE International Conference on Electronics, Circuits and Systems (ICECS 2000). December 2000. Kaslik, Lebanon: IEEE, 316 -319.

Kienzle, D.M., and Elder, M.C. (2003). *Recent Worms: A Survey and Trends*. Proceedings of the 2003 ACM Workshop on Rapid Malcode. 27 October 2003. Washington DC, USA: ACM, 1-10.

Kim. J.S., Kim, M.S. and Noh, B.N. (2004). *A Fuzzy Expert System for Network Forensics*. ICCSA 2004, Lecturer Notes in Computer Science 3034. Springer 2004: 175-182.

Klir, G.J. and Yuan, B. (1995). *Fuzzy Sets and Fuzzy Logic: Theory and Application*. USA: Prentice Hall Inc.

Labiod, K.B.H., Boutaba, R. and Guessoum, Z. (2000). *Network Security Management with Intelligent Agents*. IEEE/IFIP Network Operations and Managements Symposium. September 2000. Hawaii, USA: IEEE, 579-592.

Labuschagne, L. and Eloff, J.H.P. (1998). *The Use of Real-Time Risk Analysis to Enable Dynamic Activation of Countermeasures*. Elsevier Journal of Computer and Security. 17(4): 347-357.

Lai, S.C., Kuo, W.C., and Hsieh, M.C. (2004). *Defending Against Internet Worm-Like Infestations*. Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA '04). March 2004. Fukuoka, Japan: IEEE, 152-157.

Li, J., Zhang, G.Y. and Gu, G.C. (2004). *A Multi-Agent-Based Architecture for Network Attack Resistant System*. GCC 2003, Part I, Lecturer Notes in Computer Science 3032. Springer 2004: 980-983.

Lee, T.K., Yusuf, S., Luk, W., Sloman, M., Lupu, E. and Dulay, N. (2002). *Development Framework for Firewall Processors*. Proceedings of the 2002 IEEE International Conference on Field Programmable Technology. December 2002. Hongkong, China: IEEE, 352-355.

Lehtonen, S., Ahola, K., Koskinen, T., Lyijynen, M. and Pesole, J. (2003). *Roaming Active Filtering Firewall*. Proceedings of Smart Objects Conference (SOC'2003). 15-17 May 2003. Grenoble, France.

Lockwood, J.W., Neely, C., Zuver, C., Moscola, J., Dharmapurikar, S. and Lim, D. (2003). *An Extensible, System-On-Programmable-Chip, Content-Aware Internet Firewall*. FPL 2003, Lecturer Notes on Computer Science 2778. Springer 2003: 859-868.

Negnevitsky, M. (2002). *Artificial Intelligence: A Guide to Intelligent Systems*. England: Pearson Education Limited.

Newman, D. (1999). *RFC 2647 – Benchmarking Terminology for Firewall Performance*. Internet RFC/STD/FYI/BCP Archives. August 1999. Network Working Group, Request for Comments: 2647.

Ogletree, T.W. (2000). *Practical Firewalls.* USA: Que Corporation. June 2000.

Patton, S., Doss, D. and Yurick, W. (2000). *Open Source Versus Commercial Firewalls : Functional Comparison.* Proceedings of the 25th Annual IEEE Conference on Local Computer Networks. Nov 2000. LCN 2000. Tampa, Florida, USA: IEEE, 223 – 224.

Payne, C. and Markham, T. (2001). *Architecture and Applications for a Distributed Embedded Firewall*. In 17th Annual Computer Security Applications Conference. December 2001. New Orleans, LA, USA: IEEE, 329-338.

Power, R. (2002). *CSI/FBI Computer Crime and Security Survey*. Computer Security Issues and Trends. 2002. 8(1): 1-24.

Pruitt, S. (2004). *Web Attack Aims to Steal Surfers' Financial Details*. ComputerWorld. 25 June 2004. http://computerworld.com/securitytopics/security

Ranum, M.J. and Avolio, F.M. (1994). *A Toolkit and Methods for Internet Firewalls*. In the Proceedings of the Summer USENIX Conference. June 1994. Boston, Massachusetts, USA: USENIX, 37-44.

Ren, Y, Buskens, R. and Gonzales, O. (2004). *Dependable Initialization on Large-Scale Distributed Software*. Proceedings of the 2004 International Conference on Dependable Systems and Networks (DSN '04), IEEE Computer Society.

Reumann, J., Jamjoom, H. and Shin, K. (2001). *Adaptive Packet Filters*. In the Proceedings of IEEE Global Telecommunications Conference. November 2001. San Antonio, Texas, USA: IEEE, 25-29.

Robbins, D. (2001). *Common threads - Dynamic iptables firewalls.* From IBM website, updated 1 April 2001. http://www-136.ibm.com/developerworks/linux.

Ru, W.G. and Eloff, H.P. (1996). *Risk Analysis Modelling with the Use of Fuzzy Logic*. Elsevier Journal of Computer & Security. 15(3): 239-248.

Sandhu, R.S. (1993). *Lattice-Based Access Control Models*. IEEE Transactions on Computer, November 1993. 26(11): 9-19.

Seo, J., Kim, H.S., Cho, S. and Cha, S. (2004). *Web Server Attack Categorization Based on Root Causes and Their Locations*. Proceedings of the International Conference on Information Technology Coding and Computing (ITCC ’04). April 2004. Las Vegas, Nevada, USA: IEEE, 90-96.

Shakshuki, E., Luo, Z. and Gong, J. (2004). *An Agent-Based Approach to Security Service*. Elsevier Journal of Network and Computer Applications, Article In Press.

Silva, S.D., Yemini, Y. and Florissi, D. (2001). *The NetScript Active Network System*. IEEE Journal on Selected Areas in Communications, 2001. 19(3): 538-551.

Sully, B. (2005). *IPTables Firewall Script and Configuration Files for Linux 2.4.x-2.6.x*. In Malibyte website, updated 8 April 2005. http://www.malibyte.net/iptables/scripts/fwscripts.html.

Toth, T., and Kruegel, C. (2002). *Evaluating the Impact of Automated Intrusion Response Mechanism*. Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC ’02). December 2002. Las Vegas, Nevada, USA: IEEE, 301-310.

Triola, M.F. (2001). *Elementary Statistics*. Eighth Edition. USA: Addison Wesley Longman.

Venkatesan, R.M. and Bhattacharya, S. (1997). *Threat-Adaptive Security Policy*. 1997. In the International Conference for High Performance, Computing and Communications. February 1997. San Jose, CA, USA: IEEE, 525-531.

Verwoerd, T., and Hunt, R. (2002). *Policy and Implementation of an Adaptive Firewall*. Proceedings of the 10th IEEE International Conference on Networks. August 2002. Singapore: IEEE, 434-439.

White, J.E. (1996). *Telescript Technology: Mobile Agents*. In BradShaw, J. (ed): Software Agents. AAI Press/MIT Press.

Whitman, M.E. (2003). *Enemy at the Gate: Threats to Information Security*. Communications of the ACM. August 2003. 46(8): 91-95.

Wired News. (2004). *New Virus May Steal Data*. Wired News. 25 June 2004. http://www.wired.com/news/infostructure

Xian, Z., Jin, H., Liu, K., and Han, Z. (2002). *A Mobile-Agent Based Distributed Dynamic μFirewall Architecture*. Proceedings of the 9th International Conference on Parallel and Distributed Systems (ICPADS '02). December 2002. Taiwan: IEEE, 431-436.

Yen , J., Langari, R., and Zadeh, L.A. (1995). *Industrial Applications of Fuzzy Logic and Intelligent Systems.* New York, USA: IEEE Press.

Zadeh, L. (1965). *Fuzzy Sets.* Information and Control. 8(3): 338-353.

Zaki, M. and Sobh, T.S. (2004). *A Cooperative Agent-Based Model for Active Security Systems*. Elsevier Journal of Network and Computer Applications. 27 (2004): 201-220.

Zeller, C. (2004). *Craig Zeller's Firewall Scripts.* From ZDI website, updated 17 June 2004. http://www.zdi.net/Linux/firewalls.html.

Zetter, K. (2004). *Information Security News: Kazza Delivers More Than Tunes*. InfoSec News. 12 January 2004. http://www.weird.com/news/business

Zou, J., Lu, K. and Jin, Z. (2002). *Architecture and Fuzzy Adaptive Security Algorithm in Intelligent Firewall*. In the Proceedings of Military Communications Conference. October 2002. California, USA: IEEE, 1145-1149.