IMPROVING THE ALGORITHM TO DETECT INTERNET WORMS

MOHMMAD M. RASHEED

Universiti Utara Malaysia
2008

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

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

MOHMMAD M. RASHEED

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

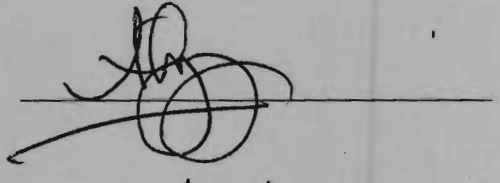
telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

IMPROVING THE ALGORITHM TO DETECT INTERNET WORMS

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 Utama
(Name of Main Supervisor): **MR. ALI YUSNY DAUD**

Tandatangan
(Signature) : 

Tarikh
(Date) : 27/5/2008

IMPROVING THE ALGORITHM TO DETECT INTERNET WORMS

This thesis is presented to the Graduate School
In fulfillment of the requirements for
Master of Science (Information Technology)
Universiti Utara Malaysia

By

MOHMMAD M. RASHEED

PERMISSION TO 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 the whole or in part, for scholarly purposes may be granted by my supervisor or in his absence, by the Dean of 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 materials for my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part should be address to:

Dean of Faculty of Information Technology
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

Abstract

Worm detection and response systems must act quickly to identify and quarantine scanning worms, as when left unchecked such worms have been able to infect the majority of vulnerable hosts on the Internet in a matter of minutes [53]. Active worm spread in an automated fashion and can flood the internet in a very short time. The aim of this project is to improved algorithm to detect internet worm by two sub algorithm. The first is detecting the internet worm and the second is detecting stealth internet worm. A new equation created for depending on the average failure connection. The study based on the comparison and analysis of many worm detection and containment strategies. The principle of this effective algorithm is an improved two rotation process to detect and contain all types of internet worms.

ACKNOWLEDGMENT

IN THE NAME OF ALLAH

Most Beneficent and Most Merciful, Praise and thanks to Allah, first and last, lord and Cherisher of all the worlds who taught humankind everything they knew. May his blessings and His Mercy be upon the holy prophet Muhammad S.A.W the best of man kind.

I would like to extend my deepest love to my family especially my parents for their loving, support and trust.

Also, I would like to thank my supervisor Mr. Ali Yusny Daud for his guidance, critique and comments. I am deeply indebted to him for his kindness and patience throughout the supervision and preparation of this research project from the start until the final stage, is invaluable to me. Words cannot express my sincere appreciation to him.

I dedicate this thesis to my mother and father.

CONTENTS

PERMISSION TO USE ..... **I**

ABSTRACT ..... **II**

ACKNOWLEDGMENT ..... **III**

CONTENTS ..... **IV**

LIST OF FIGURES ..... **VI**

LIST OF ABBREVIATION ..... **VII**

1. Introduction **1**

1.1 Overview 3

1.2 Problem Background 3

1.3 Problem Statement 4

1.4 Research Question 4

1.5 The Objective of the Study 5

1.6 Scope of Study 5

1.7 Significance 6

1.8 Organization of the Study 6

2. Literature Review **7**

2.1 Virus viruses Worm 7

2.2 Types of Computer Worms 9

3.1.1 Internet Worms 9

3.1.2 Email Worms 9

3.1.3 Instant Messaging Worms 10

3.1.4 IRC Worms 11

3.1.5 File-sharing Networks Worms 11

2.3 Worm Detection Techniques 12

2.3.1 Port-scan Technique 12

2.3.2 Honeypot Technique 12

2.3.3 Behavioral Signature Technique 12

2.4 Technique to Detect Internet Worm by Port-scan 13

2.5 Xiong Yang algorithm to Detect Internet Worm 14

2.6 Related work 15
2.7 Conclusion 17

3. Methodology..... 18
3.1 Process Steps of the Study 18
3.1.1 Awareness of the Problem..... 19
3.1.2 Suggestion 19
3.1.3 Requirement 21
3.1.4 Design 21
3.1.5 Test.....33
3.1.6 Compare the Test.....35
3.1.7 Result.....37
3.2 Conclusion.....37

4. Result..... 38
4.1 Result for Faster Detect 38
4.2 Result for Detect other Types of Worms..... 43
4.3 Conclusion.....46

5. Future work & Conclusion..... 47
5.1 Future work 47
5.2 Limitation 47
5.3 Time Schedule 48
5.4 Conclusions.....49
References 50

LIST OF FIGURES

3.1 Research Methodology..... 18
3.2 Sequence of Infected Worm..... 22
3.3 ICMP Message..... 23
3.4 RESET Message..... 23
3.5 Error Message Return to Router..... 24
3.6 Short Term & Longer Term Algorithm..... 25
3.7 Improved Algorithm to Detect Internet Worm..... 32
3.8 Test Short Term Algorithm..... 33
3.9 Test Longer Term Algorithm..... 34
3.10 Compare Two Algorithms to Detect Stealth Worm..... 35
3.11 Compare Two Algorithms to Detect Others Worm..... 36
4.1 X. Yang et al. [36] Algorithm Detect the Worm after 34min 5 sec..... 39
4.2 X. Yang et al. [36] Algorithm Detect the Worm after 32 min 15 sec..... 39
4.3 X. Yang et al. [36] Algorithm Detect the Worm after 39min 28 sec..... 40
4.4 X. Yang et al. [36] Algorithm Detect the Worm after 30min 55 sec..... 40
4.5 Improved Algorithm Detect the Worm after 103 sec..... 41
4.6 Improved Algorithm Detect the Worm after 82 sec..... 42
4.7 Improved Algorithm Detect the Worm after 3 min 1 sec..... 42
4.8 Improved Algorithm Detect the Worm after 68 sec..... 43
4.9 X. Yang et al. [36] Algorithm Can't Detect Worm after 30 hours..... 44
4.10 X. Yang et al. [36] Algorithm Can't Detect Worm after 30 hours..... 44
4.11 Improved Algorithm Detect the Worm after 30 hours..... 45
4.12 Improved Algorithm Detect the Worm after 25 hours 4 min..... 46
5.1 Research Time Schedule..... 48

LIST OF ABBREVIATION

DNS..... Domain Name System

FTP .....File Transfer Protocol

ICMP..... internet controller message protocol

IP .....Internet Protocol

IRC..... Internet Relay Chat

ITR..... Improved Two Rotation

RAM..... Random Access Memory

RATs .....Remote Access Trojans

ROM .....Read Only Memory

TCP .....Transmission Control Protocol

CHAPTER 1

INTRODUCTION

This chapter briefly explains the background of this study that mainly involves the detection internet worm. The majority of this chapter includes overview, problem statements, research questions, research objectives, scope of the study, and also significance of the research.

1.1 Overview

Currently, the internet is getting close to the persons' life. They login internet to chat with others, download files or browse WebPages. The internet is also playing an important role in the economy of country. Once the internet breaks down, it will cause an enormous economic loss. Worms is a serious security threat that may cause network congestion and internet break down.

Passive worms are different from viruses because they are completely autonomous entities. Virus is dependent upon a host file or boot sector, and the transfer of files between machines to spread, while worm can run completely independently and spread it self through network connections. An example of a worm is the famous internet worm of 1988: overnight the worm copied itself across the internet, infecting every Sun-3 and VAX system with so many copies of it self that the systems were unusable. Eventually several sites disconnected themselves from the internet to avoid reinfection [1].

A virus generally binds to executable code (both in system executables and scripts). An important part of a virus is its hiding technique, but for active worms this is not a priority since, in general, they do not piggy-back on other network protocols, meaning that worm propagation is clearly visible on the network medium. Although simple

The contents of the thesis is for internal user only

References

[1] Computer worms information, http://virusall.com/worms.shtml Accessed January 2nd, 2008.

[2] V.Berk, G.Bakos, and R. Morris, Designing a Framework for Active Worm Detection on Global Networks, In Proceedings of the IEEE International Workshop on Information Assurance, Darmstadt, Germany, March 2003.

[3] Anti-virus Policy, www.emu.org.uk/Technical/FAQs/White Papers/antiviruspolicy.doc, Accessed January 16th, 2008.

[4] D. R. Ellis, J. G. Aiken, K. S. Attwood, and S. D. Tenaglia , A Behavioral Approach to Worm Detection. Invited talk in ACM WORM 2004, page 49, Oct. 2004.

[5] M. Costa, J. Crowcroft, M. Castro, A. Rowstron,L. Zhou, L. Zhang and P. Barham ,Vigilante: End-to-End Containment of Internet Worms, In ACM, Brighton, United Kingdom.,Oct. 2005.

[6] S. Chen and Y. Tang, Slowing Down Internet Worms, Proc. of 24th International Conference on Distributed Computing Systems (ICDCS'04), Tokyo, Japan, Mar. 2004.

[7] S. E. Schechter, Fast Detection of Scanning Worm Infections. Stuart E. Schechter, and Arthur W. Berger, www.wormblog.com/2004/12.

[8] Virus, http://www.webopedia.com/TERM/v/virus.html, Accessed February15th, 2008.

[9] History of Viruses, http://www.computer-sleuth.com/history_of_viruses.htm, Accessed February15th, 2008.

[10] En.wikipedia, http://en.wikipedia.org/wiki/Computer_virus, Accessed February15th, 2008.

[11] History of computer viruses, www.antivirusworld.com/articles/history.php, Accessed February17th, 2008.

[12] History of Computer Viruses, http://www.csun.edu/~ty6255/ComputerVirus/History.html, Accessed February17th, 2008.

[13] The Social Impact of Viruses, http://www-cse.stanford.edu/classes/cs201/projects-00-01/viruses/social.html, Accessed February17th, 2008.

[14] En.wikipedia, http://en.wikipedia.org/wiki/Melissa_ (computer_worm), Accessed February18th, 2008.

[15] The Different Types of Computer Viruses, http://www.pcsecurityalert.com/pcsecurityalert-articles/different-types-of-computer-viruse.htm, Accessed February19th, 2008.

[16] Types of Computer Viruses, www.nau.edu/resnet/support/documentation/pdfs/Resnet_viruses.pdf, Accessed February19th, 2008.

[17] The different types of computer viruses, http://www.mtholyoke.edu/~rmcorriv/webproj/topic4.html, Accessed February23th, 2008.

[18] Virus hoax, http://en.wikipedia.org/wiki/List_of_computer_virus_hoaxes, Accessed February23th, 2008.

[19] En.wikipedia, http://en.wikipedia.org/wiki/Computer_worm, 2007, Accessed February23th, 2008.

[20] Computer worm, http://www.technovelgy.com/ct/content.asp?Bnum=190, Accessed February23th, 2008.

[21] C.C. Zou, D. Towsley, and W. Gong., Email Worm Modeling and Defense, 13th International Conference on Computer Communications and Networks (ICCCN'04), Chicago, USA, Oct. 2004.

[22] M. Mannan and P. C. van Oorschot., Secure public Instant Messaging: A survey. In Proceedings of the 2nd Annual Conference on Privacy, Security and Trust (PST'04), Fredericton, NB, Canada, Oct. 2004.

[23] B. Arnold, D. Chess, J. Morar, Alla Segal, M. Swimmer, An Environment for Controlled Worm Replication and Analysis, published at the Virus Bulletin, 2000.

[24] D. County, Antivirus SoftwareDefrag & File CleanupComputer, October 17 2006.

[25] J.O. Kephart, D. M. Chess, and S.R. White, Computers and Epidemiology, IEEE Spectrum, May 1993.

[26] J.O. Kephart and S.R. White, Directed-graph Epidemiological Models of Computer Viruses, Proceedings of IEEE Symposium on Security and Privacy, pp. 343–359, 1991.

[27] S. Staniford, V. Paxson, and N.Weaver, How to Own the Internet in Your Spare Time, Proceedings of the 11th USENIX Security Symposium, August 2002.

[28] Dan Ellis, Worm Anatomy and Model. Proceedings of the 2003 ACM workshop on Rapid Malcode, October 2003

[29] C. C. Zou, W. Gong, and D. Towsley, Code Red Worm Propagation Modeling and Analysis, Proceedings of 9th ACM Conference on Computer and Communications Security (CCS'02), October 2002.

[30] D. Moore, C. Shannon, G.M. Voelker, and S. Savage, Network Telescopes: Technical Report, Technical Report TR-2004-04, CAIDA, 2004.

[31] V. H. Berk, R.S. Gray, and G. Bakos, Using Sensor Networks and Data Fusion for Early Detection of Active Worms, Proceedings of the SPIE AeroSense, pp. 92–104, 2003.

[32] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank,J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle, GrIDS-a Graph Based Intrusion Detection System for Large Networks, Proceedings of the 19th National Information Systems Security Conference, October 1996.

[33] C. Zou, W. Gong, and D. Towsley, the Monitoring and Early Detection of Internet Worms, IEEE/ACM Trans. on Networking, 2005.

[34] S. Chen and Y. Tang, Slowing Down Internet Worms, Proc. of 24th International Conference on Distributed Computing Systems (ICDCS'04), Tokyo, Japan, Mar. 2004.

[35] S. E. Schechter, and A. W. Berger, Fast Detection of Scanning Worm Infections, www.wormblog.com/2004/12.

[36] X. Yang, J. Lu , Y. Zhu and P. Wang ,Simulation and Evaluation OF A New Algorithm of Worm Detection and Containment, Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies,2006.

[37] X. Jiang and D. Xu, Profiling Self-Propagating Worms via Behavioral Footprinting, ACM, November 3, 2006.

[38] H., A., M., S., P., J. and R., Design Science in Information Systems Research, MIS Quarterly 28(1): 75-105, 2004.

[39] En.wikipedia, Waterfall model, http://en.wikipedia.org/wiki/Waterfall_model Accessed January 16th, 2008.

[40] webopedia, SDLC, http://www.webopedia.com/TERM/S/SDLC.html, Accessed January 15th, 2008.

[41] M. Landesman, What is a virus, http://antivirus.about.com/cs/tutorials/a/whatisavirus.htm, Accessed march 30th, 2008.

[42] Classic Viruses, http://www.viruslist.com/en/virusesdescribed?chapter=152540474, Accessed March 30th, 2008.

[43] Computer Viruses, http://www.online.tusc.k12.al.us/tutorials/viruses/viruses.htm Accessed March 31st, 2008.

[44] Macro Viruses, http://www.ca.com/us/securityadvisor/documents/collateral.aspx?cid=33338, Accessed March 31st, 2008.

[45] Internet Worms, http://www.livinginternet.com/i/is_vir_first.htm, Accessed March 31st, 2008.

[46] M. Mannan and P. C. van, On Instant Messaging Worms, Analysis and Countermeasures, Accessed ACM, November 11, 2005.

[47] Worms and You, http://www.fws.gov/pacific/security/worms.htm, Accessed Aug, 29, 2000.

[48] Trojan Horses, http://www.ncsu.edu/resnet/viruses/trojan_horses.php, Accessed March 31st, 2008.

[49] Computer virus http://www.crews.org/curriculum/ex/compsci/articles/virusarticle.html, Accessed March 31st, 2008.

[50] Computer Viruses, http://www.fhsu.edu/int/rrohlf/WiredWest/viruses/viruses.html, Accessed March 31st, 2008.

[51] M. Hanhisalo, Computer Viruses, http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/viruses.html, Accessed March 31st, 2008.

[52] En.wikipedia, http://en.wikipedia.org/wiki/Macro_virus_(computing), Accessed February23th, 2008.

[53] M. David, P. Vern, Stefan Savage, S. Colleen, S. Stuart, and W. Nicholas, Inside the Slammer worm, IEEE Security and Privacy, July 2003.

[54] Y. Chunmei, L. Mingchu, M. Jianh and S. Jizhou, Honeypot and Scan Detection in Intrusion Detection System, IEEE, May 2004.

[55] L. Spitzner, ""Honeypots: Simple, Cost-Effective Detection", www.trackinghackers.com, May 2003.

[56] S. Singh, C. Estan, G. Varghese, and S. Savage, Automated worm fingerprinting, In Proceedings of ACM SOSP, December 2004.

[57] How to fight online Identity,

searchsecurity.techtarget.com/searchSecurity/downloads/Alagna_Ch7.pdf,

Accessed April 15th, 2008.