AN INNOVATIVE SIGNATURE DETECTION SYSTEM FOR POLYMORPHIC AND MONOMORPHIC INTERNET WORMS DETECTION AND CONTAINMENT

MOHAMMAD M. RASHEED

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2012

Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisors or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. 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 Awang Had Salleh Graduate School of Arts and Sciences

UUMCollege of Arts and Sciences

Universiti Utara Malaysia

06010 UUM Sintok

Abstrak

Kebanyakan sistem anti-cecacing dan sistem pengesanan pencerobohan terkini menggunakan teknologi berasaskan tandatangan berbanding teknologi berasaskan anomali. Teknologi berasaskan tandatangan hanya boleh mengesan serangan dengan mengenal pasti tandatangan tertentu. Sistem anti-cecacing sedia ada tidak mampu mengesan sistem jaringan Internet yang tidak diketahui dan tidak mampu melakukan pengimbasan terhadap cecacing secara automatik. Ini kerana sistem ini tidak bergantung sepenuhnya kepada tingkah laku cecacing tetapi tandatangan. Selain itu, kebanyakan algoritma pengesanan yang digunakan dalam sistem pengesanan semasa adalah mensasarkan muat beban cecacing monomorfik dan tidak mempunyai kemampuan melakukan pengesananan terhadap cecacing polimorfik, yang boleh berubah secara muatan dinamik. Sistem pengesanan anomali pula hanya mampu untuk mengesan cecacing tidak diketahui tetapi biasanya akan mempunyai kadar penggera palsu yang tinggi. Mengesan cecacing tidak diketahui adalah satu tugas yang mencabar, dan pertahanan cecacing mesti diautomasikan. Ini kerana cecacing boleh merebak terlalu cepat, yang boleh membebankan sistem jaringan Internet dalam masa yang sangat singkat. Oleh itu, kajian ini mencadangkan satu teknik yang tepat, mantap dan pantas untuk mengesan dan menampung cecacing Internet (monomorfik dan polimorfik). Teknik pengesanan menggunkan status kegagalan penyambungan protokol-protokol seperti UDP, TCP, ICMP, TCP pengimbas perlahan dan TCP pengimbas senyap sebagai ciri-ciri cecacing. Manakala pembendungan menggunakan bendera dan label pengapala segmen, sumber pelabuhan, dan destinasi pelabuhan untuk menjana tandatangan trafik cecacing. Eksperimen menggunakan lapan cecacing berbeza (monomorfik dan polimorfik) dalam persekitaran tapak uji untuk mengesahkan ketepatan dan prestasi teknik yang dicadangkan. Keputusan eksperimen menunjukkan bahawa teknik yang dicadangkan mempunyai keupayaan untuk mengesan pengimbasan sembunyi sehingga 30 kali lebih cepat daripada teknik yang dicadangkan oleh penyelidik lain, dan tidak mempunyai penggera palsu positif bagi semua kes pengesanan imbasan. Selain itu, eksperimen menunjukkan teknik yang dicadangkan adalah mampu untuk membendung cecacing disebabkan oleh hakikat keunikan tandatangan trafik tersebut.

Kata kunci: Rangkaian keselamatan, Anti-cecacing, Pengesanan anomali berasaskan cecacing, Cecacing polimorfik.

Abstract

Most current anti-worm systems and intrusion-detection systems use signature-based technology instead of anomaly-based technology. Signature-based technology can only detect known attacks with identified signatures. Existing anti-worm systems cannot detect unknown Internet scanning worms automatically because these systems do not depend upon worm behaviour but upon the worm's signature. Most detection algorithms used in current detection systems target only monomorphic worm payloads and offer no defence against polymorphic worms, which changes the payload dynamically. Anomaly detection systems can detect unknown worms but usually suffer from a high false alarm rate. Detecting unknown worms is challenging, and the worm defence must be automated because worms spread quickly and can flood the Internet in a short time. This research proposes an accurate, robust and fast technique to detect and contain Internet worms (monomorphic and polymorphic). The detection technique uses specific failure connection statuses on specific protocols such as UDP, TCP, ICMP, TCP slow scanning and stealth scanning as characteristics of the worms. Whereas the containment utilizes flags and labels of the segment header and the source and destination ports to generate the traffic signature of the worms. Experiments using eight different worms (monomorphic and polymorphic) in a testbed environment were conducted to verify the performance of the proposed technique. The experiment results showed that the proposed technique could detect stealth scanning up to 30 times faster than the technique proposed by another researcher and had no false-positive alarms for all scanning detection cases. The experiments showed the proposed technique was capable of containing the worm because of the traffic signature's uniqueness.

Keywords: Network security, Anti worm, Anomaly-based worm detection, Polymorphic worm.

Acknowledgement

I would like to express my appreciation and gratitude to everyone contributed in completing this thesis. I would like to express my thanks to my supervisors Associate Professor Dr. Osman Ghazali, Professor Dr. Rahmat Budiarto and Associate Professor Dr. Norita Md Norwawi, for their comments which help improving my work.

I would like also to give my thanks to my parents, my wife, my child, my brother, my sisters, and all of my relatives for their love and support. My goal would not have been achieved without them.

I am very grateful to Associate Professor Dr. Mazani Manaf and Dr. Massudi Mahmuddin. They were very kind during the viva. Additionally, their comments have helped to improve this work. My sincere gratitude is also due to Associate Professor Dr. Huda Ibrahim, the Dean of School of Computing. Finally, I would like to thank all of my friends for their encouragement during my study.

Declaration

Some of the works have been presented from the research reported in this thesis as listed below.

Scopus and Thomson ISI Journal Papers

[1] M. M. Rasheed, O. Ghazali, N. M. Norwawi, and M. M. Kadhum, "A Traffic Signature-based Algorithm for Detecting Scanning Internet Worms," *International Journal of Communication Networks and Information Security,* vol. 1, pp. 24-30, 2009.

[2] M. M. Rasheed, O. Ghazali, and N. M. Norwawi, "Server Scanning Worm Detection by Using Intelligent Failure Connection Algorithm," *Research Journal of Information Technology,* vol. 2, pp. 228-234, 2010.

[3] M. M. Rasheed, O. Ghazali, and N. M. Norwawi, " Intelligent Signature Detection for Scanning Internet Worms," *Information Technology Journal,* vol. 11, pp. 260-267, 2012.

[4] M. M. Rasheed, O. Ghazali, and R. Budiarto, " SYN Scanning Worm Detection," *Trends in Applied Sciences Research,* vol. 7, pp. 859-871, 2012.

[5] M. M. Rasheed, O. Ghazali, and R. Budiarto, " Fast Detection of Stealth and Slow Scanning Worms in Transmission Control Protocol," *Journal of Applied Sciences,* vol. 12, pp. 2156-2163, 2012.

Non ISI Indexed Journal Papers

[6] M. M. Rasheed, N. M. Norwawi, O. Ghazali, and M. M. Kadhum, "Intelligent Failure Connection Algorithm for Detecting Internet Worms," *International Journal of Computer Science and Network Security,* vol. 9, pp. 280-285, 2009.

[7] M. M. Rasheed, O. Ghazali, and N. M. Norwawi, "Server Worm Detection by Using Intelligent Failure Connection Algorithm," *Computer Science and Telecommunications*, vol. 27, pp. 48-52, 2010.

International Conference Papers

[8] M. M. Rasheed, M. M. Kadhum, "Improving The Failure Connection Algorithm For Detecting Unknown Internet Worms," in *International Conference on Information Technology and Multimedia*, 2008.

[9] M. M. Rasheed, M. M. Kadhum, "Traffic Signature Detection for Unknown Internet Worms," in *IEEE International Conference on Network Applications*, Protocols and Services, 2008.

[10] M. M. Rasheed, N. M. Norwawi, M. M. Kadhum and O. Ghazali, "New Generation for Intelligent Anti-Internet Worm Early System Detection," in *International Conference on Computing & Informatics*, 2009.

[11] M. M. Rasheed, N. M. Norwawi, M. M. Kadhum, and O. Ghazali, "Intelligent Anti-Internet Worm Automatically Detect and Update Signatures Server," in *International Conference on Security and Management*, 2009.

[12] M. M. Rasheed, O. Ghazali, and R. Budiarto, "Behavioural Analysis for Scanning Internet Worm," in *3rd International Conference on Engineering &ICT*, 2012.

Award

[13] O. Ghazali, M. M. Rasheed, and N. M. Norwawi, "Intelligent Internet Worm Detector," *Awarded a Bronze medal in ITEX*, 2010.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACK	Acknowledgment Flag
AFC	Average of Failure Connection
BSWD	Behavioural Scanning Worm Detection
CD	Compact Disc
CFC	Counter of Failure Connection
CICMPFC	Counter of ICMP Failure Connection
CSYNFC	Counter of SYN Failure Connection
CUDPFC	Counter of UDP Failure Connection
DAW	Distributed Anti Worm
DIPA	Destination Internet Protocol Array
DoS	Denial of Service
DPA	Destination Port Array
FCA	Failure Connections Array
FIN	Fin Flag
FTP	File Transfer Protocol
HC	History of Connection
HICMPC	History of ICMP Connections
HSYNC	History of SYN Connections
HUDPC	History of UDP Connections
ICMP	Internet Control Message Protocol
IIS	Internet Information Server
IM	Instant Messaging
IP	Internet Protocol
IPs	Internet Protocol Addresses
IPv4	Internet Protocol version 4

IW	Internet Worm
LAN	Local Area Network
MBps	Mega Byte per second
MWC	Malware Warning Center
OS	Operating System
PSH	Push Flag
RICMPNR	Record of ICMP is Not Responded
RPC	Remote Procedure Call
RST	Reset Flag
RSYNNR	Record of SYN is Not Responded
RUDPNR	Record of UDP is Not Responded
SDDSTC	Signature Detection for Destination Source Traffic Correlation
SDICMPSW	Signature Detection for ICMP Scanning Worms
SPA	Source Port Array
STCPSWD	Stealth TCP Scanning Worm Detection
SYN	Synchronize flag
SYNSWD	SYN Scanning Worm Detection
T	Threshold
TCP	Transmission Control Protocol
TSD	Traffic Signature Detection
UDP	User Datagram Protocol
UDPSWD	UDP Scanning Worm Detection
UML	Unified Modelling Language
URG	Urgent Flag
URL	Uniform Resource Locator
USB	Universal Serial Bus
WWW	World Wide Web

CHAPTER ONE
INTRODUCTION

This chapter briefly explains the background of this study. The main discussion of this chapter includes an overview, research problem, research question, research objectives, scope of study, significance of study, and organization of the thesis.

1.1 Overview

Malicious software, usually known as *malware*, is a hostile software inserted into a system to cause harm to that system or other systems [1]. Malware includes *viruses*, *worms*, *Trojan horses* and *other unwanted software* [2]. See Figure 1.1.

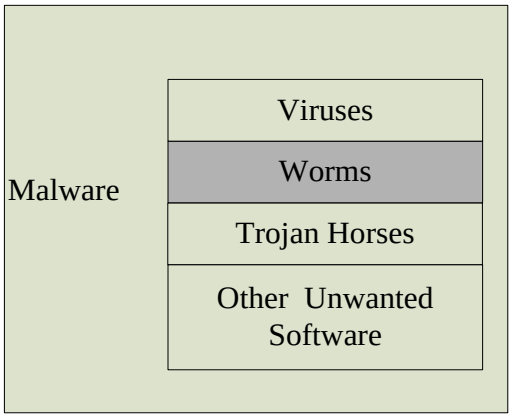

Figure 1.1: Malware Software

A computer worm is a self-replicating program working on the network. It uses a network to send copies of itself to another computer on the network, and it can do without any user's intervention [3, 4].

Worms do not need to attach themselves to an existing program, but the virus can infect other files by attaching itself to an existing program. A virus embeds itself in other executable programs while a worm is self-contained [5]. A Trojan is a program

The contents of the thesis is for internal user only

REFERENCES

[1] Y. Liang, H. Yang, T. Li, and C. Liu, "A Differential Coefficient Inspired Method for Malicious Software Detection," in *Third International Symposium on Intelligent Information Technology Application*, 2009, pp. 130-133.

[2] I. Ismail, S. M. Nor, and M. N. Marsono, "Malware Control: Issues and Challenges," in *Student Conference on Research and Development* Malaysia, 2008.

[3] S. Burji, K. J. Liszka, and C. Chan, "Malware Analysis Using Reverse Engineering and Data Mining Tools," in *International Conference on System Science and Engineering* 2010, pp. 619-624.

[4] R. Ford, "Malcode Mysteries Revealed [Computer Viruses and Worms]," *Security & Privacy, IEEE*, vol. 3, pp. 72-75, 2005.

[5] j. Yang yue and l. Wang chang, "The Spread of Malicious Software Research and Prevention," in *Second International Workshop on Education Technology and Computer Science*, 2010, pp. 777-780.

[6] J. Riordan, A. Wespi, and D. Zamboni, "How to Hook Worms [Computer Network Security]," *IEEE Spectrum*, vol. 42, pp. 32-36, 2005.

[7] Y. Tang, J. Luo, B. Xiao, and G. Wei, "Concept, Characteristics and Defending Mechanism of Worms," *IEICE Transactions on Information and Systems*, vol. E92, pp. 799-809, 2009.

[8] V. Berk, G. Cybenko, and R. Gray, "Early Detection of Active Internet Worms," in *Managing Cyber Threats*. vol. 5, V. Kumar, J. Srivastava, and A. Lazarevic, Eds., ed: Springer US, 2005, pp. 147-180.

[9] C. Xie and Z. Yin, "The Research of Worms in P2P Networks," in *International Conference on Computational Intelligence and Natural Computing*, 2009, pp. 389-392.

[10] M. Lee, T. Shon, K. Cho, M. Chung, J. Seo, and J. Moon, "An Approach for Classifying Internet Worms Based on Temporal Behaviors and Packet Flows," in *Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues*. vol. 4681, D.-S. Huang, L. Heutte, and M. Loog, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 646-655.

[11] L. Zhijun and D. Lee, "Coping with Instant Messaging Worms-Statistical Modeling and Analysis," in *15th IEEE Workshop on Local & Metropolitan Area Networks*, 2007, pp. 194-199.

[12] M. Zaki and A. Hamouda, "Design of a Multi Agent System for Worm Spreading Reduction," *Journal of Intelligent Information Systems*, vol. 35, pp. 123-155, 2010.

[13] D. Moore, C. Shannon, and k. claffy, "Code-Red: A Case Study on the Spread and Victims of an Internet Worm," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment*, Marseille, France, 2002, pp. 273-284.

[14] C. Shannon and D. Moore, "The Spread of the Witty Worm," *IEEE Security and Privacy*, vol. 2, pp. 46-50, 2004.

[15] Z. Dengyin and W. Ye, "SIRS: Internet Worm Propagation Model and Application," in *International Conference on Electrical and Control Engineering* 2010, pp. 3029-3032.

[16] J. Turnbull, P. Lieverdink, and D. Matotek, "Networking and Firewalls Pro Linux System Administration," ed: Apress, 2009, pp. 175-266.
[17] H. Noh, J. Kim, C. Y. Yeun, and K. Kim, "New Polymorphic Worm Detection Based on Instruction Distribution and Signature," in *The 2008 Symposium on Cryptography and Information Security*, Miyazaki, Japan, 2008.
[18] B. Bayoglu and İ. Sogukpinar, "Polymorphic Worm Detection Using Token-Pair Signatures," *Turkish Journal of Electrical Engineering & Computer Sciences* vol. 17, pp. 163-182, 2009.
[19] B. Rozenberg, E. Gudes, and Y. Elovici, "A Distributed Framework for the Detection of New Worm-Related Malware," in *Proceedings of the 1st European Conference on Intelligence and Security Informatics*, Esbjerg, Denmark, 2008, pp. 179-190.
[20] M. Costa, J. Crowcroft, M. Castro, A. Rowstron, L. Zhou, L. Zhang, and P. Barham, "Vigilante: End-to-End Containment of Internet Worms," *ACM SIGOPS Operating Systems Review* vol. 39, pp. 133-147, 2005.
[21] H. Jingbo, Y. Jianping, and Z. Boyun, "A Computational Model of Computer Worms Based on Persistent Turing Machines," in *5th IEEE International Conference on Cognitive Informatics* 2006, pp. 453-456.
[22] L. Tsern-Huei and L. Sung-Yen, "Adaptive Sequential Hypothesis Testing for Accurate Detection of Scanning Worms," in *TENCON 2009 - 2009 IEEE Region 10 Conference*, 2009, pp. 1-6.
[23] K. R. Rohloff and T. Basar, "Stochastic Behavior of Random Constant Scanning Worms," in *14th International Conference on Computer Communications and Networks*, 2005, pp. 339-344.
[24] A. Tikkanen and T. Virtanen, "Early Warning for Network Worms," in *Computational Intelligence and Security*. vol. 3802, Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, and Y.-C. Jiao, Eds., ed: Springer Berlin / Heidelberg, 2005, pp. 1054-1059.
[25] H. He, M. Hu, W. Zhang, and H. Zhang, "Fast Detection of Worm Infection for Large-Scale Networks," in *Advances in Machine Learning and Cybernetics*. vol. 3930, D. Yeung, Z.-Q. Liu, X.-Z. Wang, and H. Yan, Eds., ed: Springer Berlin / Heidelberg, 2006, pp. 672-681.
[26] M. Costa, J. Crowcroft, M. Castro, A. Rowstron, L. Zhou, L. Zhang, and P. Barham, "Vigilante: End-to-End Containment of Internet Worm Epidemics," *ACM Transactions on Computer Systems* vol. 26, pp. 1-68, 2008.
[27] W. Yu, X. Wang, P. Calyam, D. Xuan, and W. Zhao, "Modeling and Detection of Camouflaging Worm," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, pp. 1-1, 2010.
[28] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, "Defending against Hitlist Worms using Network Address Space Randomization," *Computer Networks*, vol. 51, pp. 3471-3490, 2007.
[29] C. Lu, "Research on Intrusion and Defense of P2P-Based Worm," in *ISECS International Colloquium on Computing, Communication, Control, and Management*, 2009, pp. 540-543.
[30] N. Jamil and T. M. Chen, "A Mathematical View of Network-Based Suppressions of Worm Epidemics," in *IEEE International Conference on Communications*, 2009, pp. 932-936

[31] L. Pele, M. Salour, and S. Xiao, "A Survey of Internet Worm Detection and Containment," *IEEE Communications Surveys and Tutorials*, vol. 10, pp. 20-35, 2008.

[32] M. M. Z. E. Mohammed, H. A. Chan, N. Ventura, M. Hashim, I. Amin, and E. Bashier, "Detection of Zero-Day Polymorphic Worms Using Principal Component Analysis," in *Sixth International Conference on Networking and Services* 2010, pp. 277-281.

[33] M. F. Zolkipli and A. Jantan, "A Framework for Malware Detection using Combination Technique and Signature Generation," in *Second International Conference on Computer Research and Development*, 2010, pp. 196-199.

[34] R. Moskovitch, C. Feher, and Y. Elovici, "A Chronological Evaluation of Unknown Malcode Detection," in *Intelligence and Security Informatics*. vol. 5477, H. Chen, C. Yang, M. Chau, and S.-H. Li, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 112-117.

[35] F. Min and R. Gupta, "Detecting Virus Mutations Via Dynamic Matching," in *IEEE International Conference on Software Maintenance*, 2009, pp. 105-114.

[36] R. Moskovitch, N. Nissim, R. Englert, and Y. Elovici, "Active Learning to Improve the Detection of Unknown Computer Worms Activity," in *11th International Conference on Information Fusion*, 2008, pp. 1-8.

[37] R. Moskovitch, I. Gus, S. Pluderman, D. Stopel, C. Feher, C. Glezer, Y. Shahar, and Y. Elovici, "Detection of Unknown Computer Worms Activity Based on Computer Behavior using Data Mining," in *IEEE Symposium on Computational Intelligence and Data Mining*, 2007, pp. 202-209.

[38] Y. Tang and S. Chen, "Defending against Internet Worms: A Signature-Based Approach," in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2005, pp. 1384-1394

[39] M. Uddin, K. Khowaja, and A. A. Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System using Mobile Agents," *International Journal of Network Security & Its Applications*, vol. 2, pp. 129-141, 2010.

[40] M. Costa, "End-to-End Containment of Internet Worm Epidemics," Churchill College, University of Cambridge, 2006.

[41] G. Blanc and Y. Kadobayashi, "Towards Learning Intentions in Web 2.0," in *4th Joint Workshop on Information Security*, Kaohsiung , Taiwan, 2009.

[42] S. Chen and Y. Tang, "DAW: A Distributed Antiworm System," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, pp. 893-906, 2007.

[43] F. C. C. Osorio and F. S. Posluszny, "Overcoming the Limitations in Computer Worm Models," in *5th International Conference on Malicious and Unwanted Software*, 2010, pp. 81-90.

[44] P. Szor, *The Art of Computer Virus Research and Defense*: Addison-Wesley Professional, 2005.

[45] Z. Mao, N. Li, H. Chen, and X. Jiang, "Trojan Horse Resistant Discretionary Access Control," in *Proceedings of the 14th ACM symposium on Access control models and technologies*, Stresa, Italy, 2009, pp. 237-246.

[46] B. Acohido and J. Swartz. (2006). *E-mail Worm Bent only on Destruction*. Available: http://www.usatoday.com/tech/news/computersecurity/2006-01-30-email-virus_x.htm, [Accessed: 1st April 2011].

[47] M. Mannan and P. C. v. Oorschot, "On Instant Messaging Worms, Analysis and Countermeasures," in *ACM workshop on Rapid malcode*, Fairfax, VA, USA, 2005.
[48] J. O. Kephart, D. M. Chess, and S. R. White, "Computers and Epidemiology," in *IEEE Spectrum*, 1993, pp. 20-26.
[49] D. County. (2006). *Antivirus Software Defrag & File CleanupComputer*. Available: http://www.uwex.edu/ces/cty/dodge/4h/projects/documents/10-17Workshop.pdf, [Accessed: 13th March 2011].
[50] Z. Hanxun, W. Yingyou, and Z. Hong, "Passive Worm Propagation Modeling and Analysis," in *International Multi-Conference on Computing in the Global Information Technology*, 2007, pp. 32-32.
[51] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "An Taxonomy of Computer Worms," in *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, 2003, pp. 11 - 18.
[52] D. Seeley, "A Tour of the Worm," in *Proceedings of 1989 Winter USENIX Conference*, San Diego, 1989, pp. 287-304.
[53] P. Y. Li, "Defending Flash Worms: Contemporary Detection Schemes and a Hierarchical Model," M.S., San Jose State University, United States California, 2006.
[54] C. C. Zou, D. Towsley, and W. Gong, "On the Performance of Internet Worm Scanning Strategies," *Performance Evaluation*, vol. 63, pp. 700-723, 2006.
[55] K. R. Rohloff and T. Basar, "Deterministic and Stochastic Models for the Detection of Random Constant Scanning Worms," *ACM: Transactions on Modeling and Computer Simulation*, vol. 18, pp. 1-24, 2008.
[56] S. H. Sellke, N. B. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, pp. 71-86, 2008.
[57] P. K. Manna, S. Chen, and S. Ranka, "Inside the Permutation-Scanning Worms: Propagation Modeling and Analysis," *IEEE/ACM Transactions on Networking*, vol. 18, pp. 858-870, 2010.
[58] Z. Chen, C. Chen, and C. Ji, "Understanding Localized-Scanning Worms," in *IEEE International Performance, Computing, and Communications Conference*, 2007, pp. 186-193.
[59] C. C. Zou, L. Gao, W. Gong, and D. Towsley, "Monitoring and Early Warning for Internet Worms," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington D.C., USA, 2003, pp. 190-199.
[60] S. Qing and W. Wen, "A Survey and Trends on Internet Worms," *Computers & Security*, vol. 24, pp. 334-346, 2005.
[61] C. C. Zou, G. Weibo, D. Towsley, and G. Lixin, "The Monitoring and Early Detection of Internet Worms," *IEEE/ACM Transactions on Networking*, vol. 13, pp. 961-974, 2005.
[62] S. Hatahet, Y. Challal, and A. Bouabdallah, "BitTorrent Worm Sensor Network : P2P Worms Detection and Containment," in *17th Euromicro International Conference on Parallel, Distributed and Network-based Processing*, 2009, pp. 293-300.
[63] D. Hati, B. Sahoo, and A. Kumar, "Adaptive Focused Crawling Based on Link Analysis," in *2nd International Conference on Education Technology and Computer* 2010, pp. 455-460.

[64] J. Hua and K. Sakurai, "Modeling and Containment of Search Worms Targeting Web Applications," in *Detection of Intrusions and Malware, and Vulnerability Assessment*. vol. 6201, C. Kreibich and M. Jahnke, Eds., ed: Springer Berlin / Heidelberg, 2010, pp. 183-199.

[65] N. Provos, J. McClain, and K. Wang, "Search Worms," in *Proceedings of the 4th ACM workshop on Recurring malcode*, Alexandria, Virginia, USA, 2006, pp. 1-8.

[66] E. Levy, "Worm Propagation and Generic Attacks," *IEEE Security and Privacy*, vol. 3, pp. 63-65, 2005.

[67] M. P. Collins, "Using Protocol Graphs to Identify Hit-List Attackers," CERT Research Annual Report 2007.

[68] J. Jung, R. Milito, and V. Paxson, "On the Adaptive Real-Time Detection of Fast-Propagating Network Worms," *Journal in Computer Virology*, vol. 4, pp. 197-210, 2008.

[69] C. Partridge and T. J. Shepard, "TCP/IP Performance over Satellite Links," *IEEE Network*, vol. 11, pp. 44-49, 1997.

[70] K. Myung-Sup, K. Hun-Jeong, H. Seong-Cheol, C. Seung-Hwa, and J. W. Hong, "A Flow-based Method for Abnormal Network Traffic Detection," in *IEEE/IFIP Network Operations and Management Symposium*, 2004, pp. 599-612

[71] J.-S. Park and M.-S. Kim, "Design and Implementation of an SNMP-Based Traffic Flooding Attack Detection System," in *Challenges for Next Generation Network Operations and Service Management*. vol. 5297, Y. Ma, D. Choi, and S. Ata, Eds., ed: Springer Berlin / Heidelberg, 2008, pp. 380-389.

[72] S. H. C. Haris, G. M. Waleed, R. B. Ahmad, and M. A. H. A. Ghani, "Anomaly Detection of IP Header Threats," *International Journal of Computer Science and Security*, vol. 4, pp. 497-504, 2011.

[73] S. Savage, N. Cardwell, D. Wetherall, and T. Anderson, "TCP Congestion Control with a Misbehaving Receiver," *ACM SIGCOMM Computer Communication Review* vol. 29, pp. 71-78, 1999.

[74] W. Jia and W. Zhou, "Internetworking," in *Distributed Network Systems*. vol. 15, ed: Springer US, 2005, pp. 65-78.

[75] P. Marques, H. Castro, and M. Ricardo, "Monitoring Emerging IPv6 Wireless Access Networks," *IEEE Wireless Communications*, vol. 12, pp. 47-53, 2005.

[76] M. Ravindran and R. Bhaskaran, "A Novel Detection of Network Errrors by Study of Raw TCP/IP Packets," in *International Conference on Computer Technology and Development*, 2009, pp. 372-376.

[77] B. A. Forouzan, *Data Communications and Networking* Four Edition: McGraw-Hill Science, 2007.

[78] G. Bakos and V. B. Early, "Early Detection of Internet Worm Activity by Metering ICMP Destination Unreachable Messages," in *Proceedings of the the SPIE Aerosense*, 2002, pp. 33-42.

[79] V. Berk, G. Bakos, and R. Morris, "Designing a Framework for Active Worm Detection on Global Networks," in *First IEEE International Workshop on Information Assurance*, 2003, pp. 13-23.

[80] J. Postel. (1981). *RFC 792 "Internet Control Message Protocol"*. Available: http://www.ietf.org/rfc/rfc792.txt, [Accessed: 2nd August 2011].

[81] J. Liebeherr and M. E. Zarki, *Mastering Networks: An Internet Lab Manual*: Addison-Wesley, 2004.
[82] M. Fukushima and S. Goto, "Analysis of TCP Flags in Congested Network," in *Internet Workshop, 1999. IWS 99*, 1999, pp. 151-156.
[83] X. Jiang and X. Zhu, "vEye: Behavioral Footprinting for Self-Propagating Worm Detection and Profiling," *Knowledge and Information Systems*, vol. 18, pp. 231-262, 2009.
[84] D. R. Ellis, J. G. Aiken, K. S. Attwood, and S. D. Tenaglia, "A Behavioral Approach to Worm Detection," in *Proceedings of the 2004 ACM workshop on Rapid malcode*, Washington DC, USA, 2004, pp. 43-53.
[85] T. Dubendorfer, M. Bossardt, and B. Plattner, "Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation," in *19th IEEE International Parallel and Distributed Processing Symposium*, 2005.
[86] M. d. Vivo, E. Carrasco, G. Isern, and G. O. d. Vivo, "A Review of Port Scanning Techniques," *ACM SIGCOMM Computer Communication Review* vol. 29, pp. 41-48, 1999.
[87] J. Messer, *Secrets of Network Cartography: A Comprehensive Guide to Nmap*: http://www.professormesser.com/, 2007.
[88] R. Hiestand, "Scan Detection Based Identification of Worm- Infected Hosts," ETHZ, Zurich: Swiss Federal Institute of Technology, 2005.
[89] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*: Insecure, 2009.
[90] W. Yuanlong, W. Chengdong, Z. Xintong, L. Bingyang, and Z. Yunzhou, "An Embedded Wireless Transmission System Based on the Extended User Datagram Protocol (EUDP)," in *2nd International Conference on Future Computer and Communication*, 2010, pp. 690-693.
[91] T. Nakayama. (2007). *W32.Sasser.Worm*. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2004-050116-1831-99&tabid=2, [Accessed: 16th January 2011].
[92] Z. Qianli, W. Jilong, and L. Xing, "Correlation Based Analysis of Spreading Codered Worms," in *International Conference on Intelligent Control and Information Processing*, 2010, pp. 458-462.
[93] J. Canavan. (2007). *W32.Dabber.A*. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2004-051414-5013-99, [Accessed: 17th January 2011].
[94] J. Oberheide, M. Goff, and M. Karir, "Flamingo: Visualizing Internet Traffic," in *10th IEEE/IFIP Network Operations and Management Symposium*, 2006, pp. 150-161.
[95] K. Ravindran and S. T. Chanson, "Failure Transparency in Remote Procedure Calls," *IEEE Transactions on Computers*, vol. 38, pp. 1173-1187, 1989.
[96] S. E.Eugene, "The MSBlaster Worm: Going from Bad to Worse," *Network Security*, vol. 2003, pp. 4-8, 2003.
[97] C. Wong, S. Bielski, A. Studer, and C. Wang, "On the Effectiveness of Rate Limiting Mechanisms," in *8th International Symposium on Recent Advances in Intrusion Detection* 2005.
[98] F. Perriot. (2007). *W32.Welchia.Worm*. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2003-081815-2308-99&tabid=2, [Accessed: 17th January 2011].
[99] A. D. Orebaugh and G. Ramirez, *Ethereal Packet Sniffing*: Syngress Publishing, 2003.

[100] I. Hamadeh, J. Hart, G. Kesidis, and V. Pothamsetty, "A Preliminary Simulation of the Effect of Scanning Worm Activity on Multicast," in *Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation*, 2005, pp. 191-198.

[101] K. Hayashi. (2007). *W32.Protoride.Worm*. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2004-011618-0828-99, [Accessed: 17th January 2011].

[102] N. Hindocha. (2007). *W32.HLLW.Raleka*. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2003-082811-4826-99, [Accessed: 17th January 2011].

[103] H.-A. Kim and B. Karp, "Autograph: Toward Automated, Distributed Worm Signature Detection," in *in the Proceedings of the 13th Usenix Security Symposium* San Diego, 2004.

[104] J. Newsome, B. Karp, and D. Song, "Polygraph: Automatically Generating Signatures for Polymorphic Worms," in *IEEE Symposium on Security and Privacy*, 2005, pp. 226-241.

[105] B. Bayoglu and I. Sogukpinar, "Polymorphic Worm Detection Using Token-Pair Signatures," in *Proceedings of the 4th international workshop on Security, privacy and trust in pervasive and ubiquitous computing*, Sorrento, Italy, 2008, pp. 7-12.

[106] D. R. Ellis, "A Behavioral Approach to Worm Detection," Ph.D. dissertation, George Mason University, United States, Virginia, 2006.

[107] K. Chong, H. Song, and S. Noh, "Traffic Characterization of the Web Server Attacks of Worm Viruses," in *Computational Science -ICCS 2003*. vol. 2658, P. Sloot, D. Abramson, A. Bogdanov, Y. Gorbachev, J. Dongarra, and A. Zomaya, Eds., ed: Springer Berlin / Heidelberg, 2003, pp. 681-681.

[108] J. Nazario, *Defense and Detection Strategies against Internet Worms*: Boston:Artech House, 2004.

[109] J. Daniel J. Sanok, "An Analysis of How Antivirus Methodologies are Utilized in Protecting Computers from Malicious Code," in *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, Kennesaw, Georgia, 2005, pp. 142-144.

[110] X. Yang, Y. Shi, and H. Zhu, "Detection and Location Algorithm against Local-Worm," *Science in China Series F: Information Sciences*, vol. 51, pp. 1935-1946, 2008.

[111] X. Bin, C. Wei, H. Yanxiang, and E. H. M. Sha, "An Active Detecting Method Against SYN Flooding Attack " in *11th International Conference on Parallel and Distributed Systems*, 2005, pp. 709-715 Vol. 1.

[112] S. H. C. Haris, R. B. Ahmad, and M. A. H. A. Ghani, "Detecting TCP SYN Flood Attack Based on Anomaly Detection," in *Second International Conference on Network Applications Protocols and Services* 2010, pp. 240-244.

[113] V. Berk, R. Gray, and G. Bakos, "Using Sensor Networks and Data Fusion for Early Detection of Active Worms," in *2003 SPIE Aerosense Conference*, Orlando, FL, 2003, pp. 92–104.

[114] Y. Xiong, L. Jing, Z. Yuguang, and W. Ping, "Simulation and Evaluation of a New Algorithm of Worm Detection and Containment," in *Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2006, pp. 448-453.

[115] G. Gu, M. Sharif, X. Qin, D. Dagon, W. Lee, and G. Riley, "Worm Detection, Early Warning and Response Based on Local Victim Information," in *Proceedings of the 20th Annual Computer Security Applications Conference*, 2004, pp. 136-145.
[116] R. McGrew, "Experiences with Honeypot Systems: Development, Deployment, and Analysis," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, 2006.
[117] W. Harrop and G. Armitage, "Defining and Evaluating Greynets (Sparse Darknets)," in *The IEEE Conference on Local Computer Networks*, 2005, pp. 344-350.
[118] N. Sarnsuwan, C. Charnsripinyo, and N. Wattanapongsakorn, "A New Approach for Internet Worm Detection and Classification," in *6th International Conference on Networked Computing*, 2010, pp. 1-4.
[119] J. W. Seifert, "Data Mining: An Overview," RL31798, 2004.
[120] M. M. Rasheed, N. M. Norwawi, O. Ghazali, and M. M. Kadhum, "Intelligent Failure Connection Algorithm for Detecting Internet Worms," *International Journal of Computer Science and Network Security,* vol. 9, pp. 280-285, 2009.
[121] R. Dantu, J. Cangussu, and A. Yelimeli, "Dynamic Control of Worm Propagation," in *International Conference on Information Technology: Coding and Computing*, 2004, pp. 419-423 Vol.1.
[122] Snort. (2011). Available: http://www.snort.org, [Accessed: 24th March 2011].
[123] M. Anbar, S. Manickam, A.-S. Hosam, K.-S. Chai, B. Baklizi, and A. Almomani, "Behaviour Based Worm Detection and Signature Automation," *Journal of Computer Science,* vol. 7, pp. 1724-1728, 2011.
[124] X. Fan and Y. Xiang, "Defending against the Propagation of Active Worms," *The Journal of Supercomputing,* vol. 51, pp. 167-200, 2010.
[125] D. J. Malan and M. D. Smith, "Exploiting Temporal Consistency to Reduce False Positives in Host-Based, Collaborative Detection of Worms," in *Proceedings of the 4th ACM workshop on Recurring malcode*, Alexandria, Virginia, USA, 2006, pp. 25-32.
[126] I. Reinhartz-Berger and A. Sturm, "Enhancing UML Models: A Domain Analysis Approach," *Journal of Database Management*, vol. 19, pp. 74-94, 2008.
[127] I. Schinz, T. Toben, C. Mrugalla, and BerndWestphal, "The Rhapsody UML Verification Environment," in *International Conference on Software Engineering and Formal Methods*, 2004, pp. 174–183.
[128] B. Unhelkar, *Verification and Validation for Quality of UML 2.0 Models*: Wiley-Interscience, 2005.
[129] A. Dedeke and B. Lieberman, "Qualifying Use Case Diagram Associations," *Computer*, vol. 39, pp. 23-29, 2006.
[130] G. Li and B. Wang, "SysML Aided Safety Analysis for Safety-Critical Systems Artificial Intelligence and Computational Intelligence." vol. 7002, H. Deng, D. Miao, J. Lei, and F. Wang, Eds., ed: Springer Berlin / Heidelberg, 2011, pp. 270-275.
[131] L. Xuandong and J. Lilius, "Checking Compositions of UML Sequence Diagrams for Timing Inconsistency," in *Seventh Asia-Pacific Software Engineering Conference*, 2000, pp. 154-161.

[132] leetupload.com. (2011). Available: http://www.leetupload.com/dbindex2/index.php?dir=Virii/Win32/Worms/&sort=filename&sort_mode=d, [Accessed: 19th June 2011].
[133] T. H. Cormen, C. Stein, R. L. Rivest, and C. E. Leiserson, *Introduction to Algorithms*: McGraw-Hill Higher Education, 2001.
[134] T. Bartz-Beielstein, M. Chiarandini, L. Paquete, and M. Preuss, *Experimental Methods for the Analysis of Optimization Algorithms*: Springer-Verlag New York, Inc., 2010.
[135] K. Yaqub, "Modeling Security Requirements of Target of Evaluation and Vulnerabilities in UML," Master, Business Administration and Social Sciences / Information Systems Sciences, Luleå tekniska universitet 2006.
[136] wireshark. (2011). Available: http://www.wireshark.org/, [Accessed: 29th March 2011].
[137] T. Holz, "Learning More About Attack Patterns With Honeypots," in *Sicherheit*, 2006, pp. 30-41.
[138] S. Reddy, S. L, and C. Prasad, "Analysis and Design of Enhanced HTTP Proxy Cashing Server," *International Journal of Computer Technology and Applications*, vol. 2, pp. 537-541, 2011.
[139] J. Yu, H. Lee, B. Lee, M. Kim, and D. Park, "Traffic Flooding Attack Detection and Classification with SNMP MIB via SVDD and Sparse Representation," in *Internetional Conference on Information System, Computer Engineering & Application*, 2011, pp. 26-34.
[140] M. Costa, M. Castro, L. Zhou, L. Zhang, and M. Peinado, "Bouncer: Securing Software by Blocking Bad Input," *ACM SIGOPS Operating Systems Review* vol. 41, pp. 117-130, 2007.
[141] R. Moskovitch, Y. Elovici, and L. Rokach, "Detection of Unknown Computer Worms Based on Behavioral Classification of the Host," *Computational Statistics and Data Analysis*, vol. 52, pp. 4544-4566, 2008.
[142] L. C. Paul, "Code Red: A Field Study of a Worm in the Wild," *Global Information Assurance Certification Paper*, 2001.
[143] A. Orebaugh, G. Morris, E. Warnicke, and G. Ramirez, *Real World Packet Captures*. Rockland: Syngress, 2004.