BACKDOOR ATTACK DETECTION BASED ON STEPPING STONE DETECTION APPROACH

KHALID ABDULRAZZAQ ABDULNABI AL-MINSHID

UNIVERSITI UTARA MALAYSIA

2014

Backdoor Attack Detection Based on Stepping Stone Detection Approach

A dissertation submitted to Dean of Research and Postgraduate Studies Office

in partial Fulfillment of the requirement for the degree

Master of Science (Information Technology)

Universiti Utara Malaysia

By

Khalid Abdulrazzaq Abdulnabi Al-Minshid

Permission to Use

In presenting this dissertation in fulfilment of the requirements for a Master of Science in Information Technology (MSc. IT) 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 dissertation in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor 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 dissertation 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 dissertation.

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

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

Abstract

Network intruders usually use a series of hosts (stepping stones) to conceal the tracks of their intrusion in the network. This type of intrusion can be detected through an approach called Stepping Stone Detection (SSD). In the past years, SSD was confined to the detection of only this type of intrusion. In this dissertation, we consider the use of SSD concepts in the field of backdoor attack detection. The application of SSD in this field results in many advantages. First, the use of SSD makes the backdoor attack detection and the scan process time faster. Second, this technique detects all types of backdoor attack, both known and unknown, even if the backdoor attack is encrypted. Third, this technique reduces the large storage resources used by traditional antivirus tools in detecting backdoor attacks. This study contributes to the field by extending the application of SSD-based techniques, which are usually used in SSD-based environments only, into backdoor attack detection environments. Through an experiment, the accuracy of SSD-based backdoor attack detection is shown as very high.

Keywords: Stepping stone, stepping stone detection, backdoor, hacker, intrusion

Acknowledgement

"In the name of Allah the Most Beneficent and Most Merciful"

All praises and thanks to the Almighty, Allah (SWT), who helps me to finish this dissertation. Allah gives me the opportunity, strength and the ability to complete my study for Master degree after a long time of continuous work. No volume of words is enough to express my gratitude towards my supervisor, Dr. Mohd Nizam Omar, who has been very concerned and gave me many interesting, valuable and sincere feedbacks throughout his supervision. Indeed, I found in his experience the main reference of my research, I greatly benefited from his detailed comments and insights that helped me clarify ideas in "Backdoor Attack Detection Based on Stepping Stone Detection Approach".

I sincerely thanks to my evaluators, Dr. Shahrudin bin Awang Nor and Dr. Ahmad Suki Bin Che Mohamed Arif, and thanks to Dr. Mohd. Hasbullah bin Omar, Prof. Madya Dr. Faudziah Bt Ahmad, Dr. Nooraini Binti Yusoff, and other committee members, for graciously reviewing this work and giving valuable suggestion and comments on my work. I would also like to say a big thanks to all UUM lecturers and staff members at the School of Computing who were kind enough to give me their precious time and assistance, without which I would not have been able to complete this Master's dissertation. I am indebted and thankful to all Malaysian people who are very friendly and make us feel that we are not strangers in Malaysia. Last but not least, the words cannot express my gratitude to my family, especially my mother, my dear brothers Salam, Hamid and Wissam, my sisters, my faithful wife, my sons Ahmed and Murtdha and my five daughters, Duha, Saja, Nor, Tbark and Baneen. Words cannot describe their constant love, care, concern, patience, throughout the two years of my study abroad. I'm forever thankful, grateful, and indebted to them. I dedicate the accomplishment of this dissertation to my father, may Allah bless him!, my affectionate mother, and to the twin of my spirit, my wife.

"Thank you UUM"

Khalid Al-Minshid

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER ONE
INTRODUCTION

1.1 Introduction

Network applications are an important part of our daily lives. We cannot dispense with the use of these networks. At the same time, security attacks have been dramatically increasing. Security attacks come from users who do not have authorization to access the network and use the software. Most of the time, an unauthorized access is run by using a special malicious software called "malware."

In the last ten years, malware attacks have become a common crime story online. Nowadays, well-known threats, including viruses, worms, trojans, backdoors, exploits, password stealers, and spyware, have reached millions, and among these threats, the backdoor attack has a high rate of intrusion across global networks around the world (Microsoft, 2012).

The backdoor attack is a hidden technique used to gain remote access to a machine or another system without authentication. It was a major threat in recent years and is one of the threats that cause serious concerns because the outbound it generates consists of several types of packages and exerts dangerous control over a range of hosts (B. Choi & Cho, 2012). As such, detecting backdoors has become an urgent demand today.

The contents of the thesis is for internal user only

REFERENCES

Agrawal, H., Alberi, J., Bahler, L., Conner, W., Micallef, J., Virodov, A., & Snyder, S. R. (2010). *Preventing insider malware threats using program analysis techniques.* Paper presented at the MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010.

Balzarotti, D., Cova, M., Karlberger, C., Kruegel, C., Kirda, E., & Vigna, G. (2010). *Efficient detection of split personalities in malware.* Paper presented at the Network and Distributed System Security Symposium (NDSS).

Banerjee, U., Vashishtha, A., & Saxena, M. (2010). Evaluation of the Capabilities of WireShark as a Tool for Intrusion Detection. *International Journal of Computer Applications, 6*(7).

Borders, K., Zhao, X., & Prakash, A. (2006). *Siren: Catching evasive malware.* Paper presented at the Security and Privacy, 2006 IEEE Symposium on.

Choi, B., & Cho, K. (2012). Detection of Insider Attacks to the Web Server. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 3*(4), 35-45.

Choi, W. S., & Choi, S. G. (2013). *An enhanced method for mitigation of network traffic using TCP signalling control.* Paper presented at the Advanced Communication Technology (ICACT), 2013 15th International Conference on.

Crawford, M., & Peterson, G. (2013). *Insider Threat Detection using Virtual Machine Introspection.* Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Decloedt, H. E., & Van Heerden, R. (2010). Rootkits, Trojans, backdoors and new developments.

Dittmann, J., Karpuschewski, B., Fruth, J., Petzel, M., & Munder, R. (2010). *An exemplary attack scenario: threats to production engineering inspired by the Conficker worm.* Paper presented at the Proceedings of the First International Workshop on Digital Engineering.

G. T. I. S. Center. (n.d.). Open Malware Retrieved July 13 2013, from http://oc.gtisc.gatech.edu:8080

Gribble, S., Levy, H., Moshchuk, A., & Bragin, T. (2013). Detection of spyware threats withn virtual machine. : US Patent 20,130,014,259.

Idika, N., & Mathur, A. P. (2007). A survey of malware detection techniques. *Purdue University*, 48.

Kampasi, A., Zhang, Y., Di Crescenzo, G., Ghosh, A., & Talpade, R. (2007). *Improving stepping stone detection algorithms using anomaly detection techniques*.

Kang, B., Kim, H. S., Kim, T., Kwon, H., & Im, E. G. (2011). *Fast malware family detection method using control flow graphs.* Paper presented at the Proceedings of the 2011 ACM Symposium on Research in Applied Computation.

Kuo, Y.-W., & Huang, S.-H. (2008). *An Algorithm to Detect Stepping-Stones in the Presence of Chaff Packets.* Paper presented at the Parallel and Distributed Systems, 2008. ICPADS'08. 14th IEEE International Conference on.

Kurose, J. F., & Ross, K. W. (2012). *Computer networking*: Pearson Education.

Li, P. (2011). *Detecting stepping stones in internet environments*. Victoria: Deakin University.

Li, P., Zhou, W., & Wang, Y. (2010). *Getting the real-time precise round-trip time for stepping stone detection*. Paper presented at the Network and System Security (NSS), 2010 4th International Conference on.

Maarof, M. A., & Osman, A. H. (2012). Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph. *American Journal of Applied Sciences, 9*.

Menahem, E., Shabtai, A., Rokach, L., & Elovici, Y. (2009). Improving malware detection by applying multi-inducer ensemble. *Computational Statistics & Data Analysis, 53*(4), 1483-1494.

Microsoft. (2012). Microsoft Security Intelligence Report *"WORLDWIDE THREAT ASSESSMENT"* (Vol. 13): Technical Report.

Mila. (2013). Contagio Malware Dump Retrieved Sep 30, 2013, from http://contagiodump.blogspot.com/2013/04/collection-of-pcap-files-from-malware.html#more

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2012). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*.

Mohan, R. (2013). Network Analysis and Application Control Software based on Client-Server Architecture. *arXiv preprint arXiv:1304.5015*.

Mudzingwa, D., & Agrawal, R. (2012). *A study of methodologies used in intrusion detection and prevention systems (IDPS)*. Paper presented at the Southeastcon, 2012 Proceedings of IEEE.

NETRESEC. (2010, 2013). NETRESEC Retrieved November, 01, 2013, from http://www.netresec.com

Ni, L., Yang, J., Zhang, R., & Song, D. (2008). *Matching TCP/IP Packets to Resist Stepping-Stone Intruders' Evasion.* Paper presented at the System Theory, 2008. SSST 2008. 40th Southeastern Symposium on.

Omar, M. N. (2005). *The Optimization of Stepping Stone Detection Algorithm in Intrusion Detection System* Master Universiti Teknologi Malaysia, Skudai, Johor,.

Omar, M. N. (2011). *Approach for Solving Active Perturbation Attack problem in Stepping Stone Detection*. PHD, Universiti Sains Malaysia, Malaysia (USM) Penang.

Omar, M. N., Amphawan, A., & Din, R. (2012). Evolution of Stepping Stone Detection and Emerging Applications. *11 WSEAS International Conference on Information Security and Privacy (ISP'12)*.

Omar, M. N., Amphawan, A., & Din, R. (2013). A Stepping Stone Perspective to Detection of Network Threats.

Paxson, V., & Zhang, Y. (2000). *Detecting backdoors*. Paper presented at the Proc. of 9th USENIX Security Symposium.

Ping, L., Wanlei, Z., & Yini, W. (2010, 1-3 Sept. 2010). *Getting the Real-Time Precise Round-Trip Time for Stepping Stone Detection.* Paper presented at the Network and System Security (NSS), 2010 4th International Conference on.

Prasad, M. S., Babu, A. V., & Rao, M. K. B. (2013). An Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms. [International Journal of Computer Science and Management Research]. *International Journal of Computer Science and Management Research, 2*.

Radmand, A. (2009). A ghost in software Retrieved sep, 21, 2013, from http://cs.columbusstate.edu/cae-ia/StudentPapers/radmand.azadeh.pdf

Salimi, E., & Arastouie, N. (2011). *Backdoor Detection System Using Artificial Neural Network and Genetic Algorithm.* Paper presented at the Computational and Information Sciences (ICCIS), 2011 International Conference on.

Sathyanarayan, V., Kohli, P., & Bruhadeshwar, B. (2008). *Signature generation and detection of malware families.* Paper presented at the Information Security and Privacy.

Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. (2012). "Andromaly": a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems*, 1-30.

Shullich, R., Chu, J., Ji, P., & Chen, W. (2011). A Survey of Research in Stepping-Stone Detection. *International Journal of Electronic Commerce, 2*(2).

Siddiqui, M., Wang, M. C., & Lee, J. (2008). *A survey of data mining techniques for malware detection using file features.* Paper presented at the Proceedings of the 46th Annual Southeast Regional Conference on XX.

Sobh, T. (2008). *Novel algorithms and techniques in telecommunications, automation and industrial electronics*: Springer.

Sonawane, S., Prasad, G., & Pardeshi, S. (2012). A survey on intrusion detection techniques. *World Journal of Science and Technology, 2*(3).

Soni, C. (2013). Capturing of HTTP protocol packets in a wireless network. *International Journal of Wired and Wireless Communications, 1*(2), 5-10.

Sukwong, O., Kim, H. S., & Hoe, J. C. (2011). Commercial antivirus software effectiveness: an empirical study. *Computer*, 63-70.

Tahan, G., Rokach, L., & Shahar, Y. (2012). Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features. *The Journal of Machine Learning Research, 98888*, 949-979.

Virustotal. (2013). VirusTotal Retrieved July 13, 2013, from https://www.virustotal.com/

VMware. Inc. (2013). VMware software Retrieved Oct 19, 2013, from https://www.vmware.com/ap

W. Foundation. (2013). Wireshark Retrieved July 13, 2013, from http://www.wireshark.org/

Waksman, A., & Sethumadhavan, S. (2011). *Silencing hardware backdoors*. Paper presented at the Security and Privacy (SP), 2011 IEEE Symposium on.

Wang, X., & Reeves, D. (2011). Robust correlation of encrypted attack traffic through stepping stones by flow watermarking. *Dependable and Secure Computing, IEEE Transactions on, 8*(3), 434-449.

Welch, V., Pearson, D., Tierney, B., & Williams, J. (2012). Security at the Cyber Border: Exploring Cybersecurity for International Research Network Connections.

Wu, H.-C., & Huang, S.-H. (2007). *Detecting stepping-stone with Chaff perturbations*. Paper presented at the Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on.

Yang, J., & Lee, B. (2008). Detecting Stepping-Stone Intrusion and Resisting Evasion through TCP/IP Packets Cross-Matching *Autonomic and Trusted Computing* (pp. 2-12): Springer.

Zhang, Y., & Paxson, V. (2000). *Detecting stepping stones*. Paper presented at the Proceedings of the 9th USENIX Security Symposium.

PUBLICATIONS

1) Alminshid, K., & Omar, M. N. (2013, 23-25 Sept). *Detecting backdoor using stepping stone detection approach.* Paper presented at the Informatics and Applications (ICIA), 2013 Second International Conference on, Lodz, Poland, published by the IEEE Xplore, index by the (ICIA),2013 Second International Conference Proceeding.

2) Basha, A. D., Mnaathr, S. H., Alminshid, K., & Umar, I. N. (2013). Importance Applications Mobile Agent technology for Virtual E-learning Environment: Proposed Model. *International Journal of Enhanced Research in Science Technology & Engineering, 2*(5), (24-28), 2319-7463.

3) Mnaathr, S. H., Basha, A. D., Alminshid, K., & Jamaludin, R. (2013). The Opportunities and Difficulties for M-learning to Enhancing students learning results. *International Journal of Enhanced Research in Science Technology & Engineering, 2*(5), (24-28), 2319-7463.