COMPARISON OF PATTERN MATCHING ALGORITHM FOR ENHANCING SNORT PERFORMANCE

ABUBAKAR ABDULKADIR

A project submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2013

This dissertation is dedicated to my beloved wife for her endless support and encouragement, and to my parents.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude and my sincere appreciation to my supervisor **Professor Dr. Mohd Aizaini Maarof** and my co-supervisor **Assoc. Professor Dr. Suleiman Ibrahim** for their constant support, encouragement, guidance and friendship. They inspired me greatly to work in this project. Their willingness to motivate me contributed tremendously to our project. I also like to express my sincere gratitude to the course co-ordinator **Dr. Anazida** whose words of courage has prepared me to truly face the challenges encountered during my studies.

Besides, I would like to express my sincere gratitude to my parents, Mallam Usman Mai-Katsina and Mallam Umar Dahiru Malumfashi for their constant courage and prayers which have no doubt grantee my success in my studies. Also I acknowledge the effort of my wife and my kids for the lone less situation they found themselves during my studies. Finally, I like to thanks all my friends that have assisted me during my study.

ABSTRACT

Nowadays, intrusion detection system has become widely used as a network perimeter security. The used of IDS to deter the massively sophisticated attacks in most of our industries, governmental organization and educational institutions .However ,Intrusion detection system can be either host-based or network based intrusion detection system, in a host-base intrusion it monitors the host where its configured while the network-based IDS it monitors both inbound and outbound traffic network. In addition, signature based or anomaly based detection techniques are used to detect anomalous packets or attack in both network and host-based intrusion detection systems. Therefore, the challenges faced by most of the signature based detection systems e.g. snort tool is inability to detect malicious traffic at higher traffic network, which resulted in a packet drooping and subjected the network where this signature based system is configured as a network perimeter security. The challenges resulted as a result of inefficiency of the pattern matching algorithms to efficiently perform pattern matching. In addition, this research work aim to compare the current modified Boyer Moore pattern matching algorithm used by the snort IDS with the Native pattern matching algorithm in order to evaluate their performance and recommend for the implementation of the new pattern matching algorithm that will enhance snort detection performance.

ABSTRAK

Kini, sistem pengesanan pencerobohan telah menjadi digunakan secara meluas sebagai keselamatan perimeter rangkaian. Digunakan IDS untuk menghalang serangan secara besar-besaran canggih dalam kebanyakan industri kami, pertubuhan bukan kerajaan dan institusi pendidikan. Walau bagaimanapun, sistem pengesanan pencerobohan boleh sama ada berasaskan hos atau sistem pengesanan pencerobohan berasaskan rangkaian, pencerobohan pelbagai asas ia memantau tuan rumah mana dikonfigurasi manakala IDS berasaskan rangkaian ia memantau trafik rangkaian kedua-dua masuk dan keluar. Di samping itu, tandatangan berasaskan atau anomali pengesanan teknik berasaskan digunakan untuk mengesan paket ganjil atau serangan dalam rangkaian dan sistem pengesanan pencerobohan berasaskan hos. Oleh itu, cabaran yang dihadapi oleh kebanyakan sistem pengesanan tandatangan berasaskan contohnya alat mendengus adalah ketidakupayaan untuk mengesan trafik berniat jahat pada rangkaian trafik yang lebih tinggi, yang menyebabkan paket melabuh dan memudahkan rangkaian di mana sistem ini berasaskan tandatangan dikonfigurasi sebagai keselamatan perimeter rangkaian. Cabaran menyebabkan sebagai akibat daripada ketidakcekapan corak sepadan algoritma untuk cekap melaksanakan pemadanan corak. Di samping itu, matlamat ini kerja penyelidikan untuk membandingkan yang diubahsuai semasa Boyer Moore corak algoritma padanan yang digunakan oleh IDS mendengus dengan corak asli sepadan algoritma untuk menilai prestasi mereka dan mencadangkan untuk pelaksanaan Algoritma padanan corak baru yang akan meningkatkan pengesanan mendengus prestasi.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Overview

In the current network age, the security issues is the most paramount research topic in networking, securing network boundaries using intrusion detection system ensures maintenance of many company assets and ensures the services reliability as such many companies and organizations spends more in security in order to maintained their services. However, as a result of vast increase in technology and lack of integrating good security practice in software and hardware design which has leads to backdoors, bugs and e.t.c. A number of network attacks are increasing dramatically, ranging from denial of services, IP spoofing eavesdropping, mitnick, (MITM) man in the middle attack masquerading and malware attacks (Snehal and Jadhav,2010). These attacks have made traditional network security mechanism ineffective, which requires additional defense mechanism that can analyze, detect and mitigate these attacks.

However, in order to address these challenges, intrusion detection system is now widely used as a network perimeter security. Intrusion detection has been almost studied nearly 20 years back (Ning and Jajodia, 2001). Intrusion detection system is deployed in conjunction with other security mechanism to provide a better network defense against unauthorized access by user and malicious code attacks. However,

several reasons make deployment of intrusion detection system to be unavoidably part of the entire defense system. Many systems and applications are deployed without much security consideration and due to lack of good security practices in computer related application design.

Moreover, a lot of different open source and commercial intrusion detection systems are in existence, the different types of intrusion detection systems depend on the nature of the environment where these systems are deployed, either through Network-based intrusion detection systems or Host-based intrusion detection system. The other categories of intrusion detection system are based on the techniques used in identifying network intrusion. The two major techniques include misuse and anomaly detection. However, signature-based detection techniques are used to identify malicious packet or code by matching the packet payload with the pre-defined signature stored on the system data base. This technique is considered as techniques used for detecting usually malicious packet or malware but despite its good quality in detection accuracy it present performance degradations when subjected in a higher traffic network (Salah and Kahtani, 2009). The performance limitation has lead to many problems associated with systems using signature based as a techniques for intrusion detection which includes packet dropping that happen as a result of excessive string processing by the pattern matching algorithm which nearly took almost 40% to 50% of the snort processing time.

An example of signature-based technique is snort tool which also experience a higher number of packet dropping. However, snort tool is an open source intrusion detection system widely deployed in middle sized industries and most of campus networks. Because of its nature of flexible code, it has attract many researchers toward developing additional features that can meet user requirement e.g snort Mysql pre-processor plug-in to monitor communication between client and mysql server and to be able to detect any anomalous packets (Geddes and Linda, 2009).

1.2 Problem Backgrounds

University of technology Malaysia is the oldest public engineering and technology in Malaysia. The university specializes in many different technical studies such as mechanical ,Electrical and in addition computer science and information system and also the university spare a separate department that provide a services with regards to the information services with a wide range that covers the entire university and some of its colleges. The department of CCIT in the university is positioned in too many different units that ensure easy management of their service, The most important concern of this project is security unit that provides security management of the end users accounts and secured access to various information system in the university i.e .Library information system, and other management information system.

However, the deployment or configuration of intrusion detection system in a network as a perimeter security has being playing a vital roles in detecting malicious attacks that directly or indirectly disrupt the services supported by the network. However, with the recent trends in malware design, and intrusion techniques, have rendered these intrusion detection systems that used signature-based detection techniques un-useful. Moreover, the popularly used open source intrusion detection system (IDS) ie. Snort tool, which is widely deployed in most Universities and some medium size enterprises, university technology Malaysia inclusive, have being faced with so many challenges which had made most of the networks where snort intrusion detection is deployed or configured as a intrusion detecting mechanism vulnerable to various malicious attacks, i.e.

Malware, virus, Trojan horses, denial of service attack, web attack, and many other, this is as a result of the limitations of signature-based detection techniques used by the snort IDS and performance degradation experienced when subjected to the higher traffic network. The snort performance degradation is as result of the

excessive need of processing time by the snort to matches the pre-defined signature exists in its database and the Pattern of the packets. Similarly, the in ability of the snort pattern matching algorithm to perform deep packet inspection efficiently at the required network speed present a lot of threats to the network where snort configured as network perimeter security such as packet dropping and algorithmic attacks.

1.3 Problem Statement

Most of the intrusion detection systems deployed by the IT-based business companies or educational institutions are either signature based techniques to detect anomalous network packet, or statistical anomaly based detections techniques. One of the well recognized signature-based technique is the snort tool. However, the use of snort tool in intrusion detections of malware has many associated factors. These factors are as follow, which has contributed to the well done inefficiency of the snort tools, some of these problems includes the following. The inability of the snort tool to detect and log unknown and known malware variants, and also obfuscated malware, also the lag time between snort repository rule update and release of new malware has contributed immensely in the downward performance of snort tool. Snort tool experiences performance degradation in higher rate traffic network which lead to the packet dropping.

The extensive use of CPU by the snort detection engine require large amount of memory and CPU usage, for the analysis of incoming packet for any malicious behaviors or match the problem associated to the Snort performance that can be upgraded by optimizing the pattern of machine algorithms. The performance of snort tool in malware detection make the network where snort is deployed as network base intrusion detection system to be highly infected by malicious software without being detected by the snort tools for the administrator to takes an appropriated action before harm is done to the network application by the malicious code. Also problem

of false alarms appears to be most pressing one. These problems have served as a catastrophe to the snort performance enhancement, which has subjected the network in to the many problems such as a dropping of packets.

Therefore, this project will focus on studying the pattern matching algorithms used by snort signature based detection system and how this algorithms contribute to the snort performance degradations and packet dropping, the project will analyzes some pattern matching algorithms and suggest one that will yield better snort performance if implemented in snort tool. However, the research question for this project addresses the following.

i. How to compare modified Boyer Moore and Native pattern matching algorithm to evaluate performance degradation and packet dropping

ii. How to compare the two algorithms in order to suggest for better performance.

iii. How to verify the suggested enhancement can improve pattern matching used by snort

1.4 Objectives of the Project

Aims of the project is to study different components of snort tools and compare between one of pattern matching algorithms and snort Modified Boyer Moore patter matching algorithm. This is in order to suggest the performance of snort tool in UTM network. Therefore, the following objectives are set to be achieved:

i. To study and compare two patterns matching algorithms that can be implemented in the snort pattern matching algorithm.
ii. To study and analyze the weaknesses and strength of snort tool Intrusion Detection System (IDS).
iii. To suggest ways to enhance the snort tool capability in intrusion detections by implementing the efficient algorithm.

1.5 Scope of the Project

The project has the following boundary to be considered in the study:

i. The study is limited to snort components and snort pattern matching Algorithms
ii. The study uses open source snort tool application.
iii. The study will aim at comparing Modified Boyer Moore and Native pattern Matching algorithm.

Also, the project data used in this work are converted hexadecimal representation of TCP to test the effect of the shift functions in M. Boyer Moore and Plain of English text.

1.6 Significance of the Project

This research project will be used to analyze the current snort performance problem courses and understand the pattern matching algorithm that can give better performance to the snort detection engine. The result of the project will be used by the University of Technology to enhance the performance of its network intrusion detection system.

1.7 Project Organization

This project is organized in chapters as follows: Chapter One (1) provide the general overview of the research topic and scope, objective and the statement of the problems while Chapter two (2) reviewed some literatures about intrusion detection system and Chapter three (3) is the methodology to be used in comparing two different pattern matching algorithm. Indeed, Chapter four (4) and five (5) presents the project initial finding and the discussions and finally Chapter (6)

REFERENCES

Abuhmed, T., Mohaisen, A., & Nyang, D. (2011). Deep Packet Inspection for IntrusionDetection Systems *A Survey. Information Security*

Alserhani, F., Akhlaq, M., Awan, I. U., Cullen, A. J., and Mellor, J. (n.d.). Snort Performance Evaluation 1. *Performance Evaluation international journal*

Alia, M. A., Hnaif, A. A., Al-anie, H. K., Abu, K., Manasrah, A. M., & Sarwar, M. I. (2011). An ovel header matching a lgorithm for, *3*(4).

Antonatos, S., Anagnostakis, K. G. Ý., Markatos, E. P., Polychronakis, M., & Street, S. (1998). Performance Analysis of Content Matching Intrusion Detection Systems

Baker, Z. K., Member, S., and Prasanna, V. K. (2005). Flexible Intrusion Detection *October, 13(10), 1179-1189.*

Bansal, K. (2008). The Knuth-Morris-Pratt algorithm.

Boob, S., and Jadhav, P. (2010). Wireless Intrusion Detection System *International Journal,5(8), 9-13.*

Brown, D. J., Suckow, B., and Wang, T. (2008). A Survey of Intrusion Detection Systems Information Sources Analysis Techniques.

Brown, D. J., Suckow, B., and Wang, T. (2007). A Survey Information Sources Analysis Techniques, *International conference*

Dhanalakshmi, Y. (2008). Intrusion Detection Using Data Mining Along Fuzzy Logic and Genetic Algorithms. *Journal of Computer Science, 8(2), 27-32*

Dı, J. (2009). Anomaly-based network intrusion detection : Techniques , systems and Challenges, *28, 18-28. doi:10.1016/j.cose.2008.08.003*

Hai-sheng, Q. I. N. (2011). Algorithm Based on Instrusion Detection System, 0-3 *International journal of computer science.*

Idika, N. (2007). A Survey of Malware Detection Techniques. *Purdue University*, 48.

Jyothsna, V., Prasad, V. V. R., & Prasad, K. M. (2011). A Review of Anomaly based Intrusion Detection Systems. *International Journal, 28(7), 26-35.*

Kumar, S. (2011). Design and Implementation of IDS Using Snort , Entropy and *Alert Ranking System. Source, (Icsccn), 264-268.* 84

Mandumula, K. K. (2011). History of Intrusion Detection System Attacks. *Internation journal of Security,*

Nazer, G. M. (2011). Current Intrusion Detection Techniques in Information Technology . A Detailed Analysis. European Journal of Scientific*Research, 65(4), 611- 624.*

Norton, M. (2002). Optimizing Pattern Matching for Intrusion Detection. System, 11.

Papadogiannakis, A., Polychronakis, M., & Markatos, E. P. (n.d.). Improving . . theAccuracy of Network Intrusion Detection Systems Under Load Using Selective Packet s Discarding.

Rajasekhar, K., Babu, B. S., Prasanna, P. L., Lavanya, D. R., & Krishna, T. V. Raju, . (2011). An Overview of Intrusion Detection System Strategies and Issues. *Network, 8491, 127-131*.

Raju, B., & Srinivas, B. (2012b). Network Intrusion Detection System Using KMP PatternMatchingAlgorithm.*ComputerScience and Telecommunications, 3(1),* .

Roozbahani, A. R. (2009). Service Oriented Approach to Improve the Power of *Snorts. doi:10.1109/ICCEE.2009.270.*

Salah, K. Ã., & Kahtani, A. (2010). Journal of Network and Computer Applications Performance evaluation comparison of Snort NIDS under Linux and Windows Server. Journal of Network and Computer Applications, 33(1), 6-15 85 *Elsevier*

Sandhu, U. A., Haider, S., Naseer, S., & Ateeb, O. U. (2011a). A Survey of Intrusion Detection & Prevention Techniques. *Management, 16, 66-71*.

Security, C., & Monitoring, T. (2011). Importance of Intrusion Detection System *(IDS). International Journal, 2(1), 1-4.*

Sedjelmaci, H., & Feham, M. (2011). novel h ybrid i ntrusion d *etection system. Network Security, 3(4), 1-14.*

Sheik, S. S., Aggarwal, S. K., Poddar, A., Balakrishnan, N., & Sekar, K. (2004). A FAST Pattern Matching Algorithm, *1251-1256*

Singhrova, A. (2011). A Host Based Intrusion Detection System for DDoS Attack in. *wlan. Engineering, 433-438.*

Singla, N., & Garg, D. (2012). String Matching Algorithms and their Applicability invarious Applications. *Soft Computing, (6), 218-222*

Snort, D. Dissecting Snort. Network. Tekniska, K. (2010.). Intrusion Detection *Systems.*

Verwoerd, T., & Hunt, R. (2002). Intrusion detection techniques and approaches. *Computer Communications, 25, 1356-1365*

Weinsberg, Y., & Dolev, D. (2009.). High Performance String Matching Algorithm for a Network Intrusion Prevention System (NIPS)s. *P And T.*

Wu, S., and Manber, U. (1994). A fast algorithm for multi-pattern searching, 1-11

Yao, B. L., and Chen, Z. (2010). A Network Intrusion Detection System with the *Snooping Agents. Source, (Iccasm), 232-236.* 86