HARDWARE FIREWALL

ABDULLAH ABDULHAMEED GUMAAN

A report submitted in partial fulfillment of the
requirements for the award of the degree of
Bachelor of Engineering (Electrical-Microelectronics)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

JULY 2012

"Specially dedicate to my beloved family, lectures and friends
for their support and encouragement throughout my education. "

ACKNOWLEDGEMENT

In the name of Almighty Allah, the most Gracious, the most Merciful, for giving me the determination and will to complete my final year project.

My deepest gratitude goes to my supervisor Dr Nadzir Bin Marsono for his valuable and close supervision, guidance, comments, resources, encouragement, motivation, inspirations and friendship rendered throughout the study. I am also very grateful to Alireza Monemi and Ismahani binti Ismail for their help, valuable advice, guidance and motivation. Without their continued support and interest, this report would not have been the same as presented here.

My heartiest and utmost gratitude goes to my dear father, mother, uncle and all my family for their patience, sacrifices, understanding, constant concern, moral support and prayers during the course of my study.

Abdullah Abdulhameed Gumaan
Skudai, Johor - Malaysia

ABSTRACT

Internet became an essential element in human life. Huge amount of data and information is transferred through the internet worldwide every second. In addition the internet bandwidth is increasing rapidly. At the same time the risk exposed to the computing equipment, data storage and the users also increasing. Firewall is a protection tool that allows a single machine or a network to connect to the Internet or to another network while providing a degree of security. Firewall systems developed based on signatures, the quality and the way these signatures generated has a huge Influence on the entire system. Older generator still produce high amount of fault signatures (true negative). Therefore, we are proposing new firewall system based on signatures matching. The signatures have high level of accuracy and automatically generated from honeypot malicious traffic. Since the hardware is the best solution to enable full matching under high speed connection, NetFPGA reference design is used to build this system. The result shows that the signatures generated are sensitive and accurate. Furthermore functional simulations prove that the NetFPGA switch reference design is suitable to realize the string matching architecture for enhanced firewall implementation.

ABSTRAK

Internet adalah elemen yang penting dalam kehidupan manusia, data dan maklumat yang jumlah besar dipindahkan melalui saluran internet di seluruh dunia setiap saat dalam setiap hari. Di samping itu, kegunaan internet seperti jalur lebar telah bertambah dengan cepat. Pada masa yang sama, risiko terdedah kepada sumber komputer, storan data dan reputasi pengguna juga meningkat. Firewall adalah suatu alat perlindungan yang membolehkan mesin tunggal atau sesuatu rangkaian yang digunnakan untuk menyambungkan Internet atau rangkaian lain dan pada masa yang sama it menyediakan suatu tahap keselamatan. Sistem firewall dibangunkan berdasarkan padanan tandatangan. Kualiti dan cara tandatangan yang dijana mempunyai pengaruh yang amat besar ke atas seluruh sistem. Penjana pada masa lepas masih menghasilkan jumlah kesalahan tandatangan (benar negatif) yang tinggi. Oleh itu, kami mencadangkan sistem firewall yang baru berdasarkan padanan tandatangan. Tandatangan mempunyai tahap ketepatan yang lebih tinggi dan dijanakan secara automatik daripada trafik honeypot yang tercemar. Oleh kerana perkakasan adalah penyelesaian yang terbaik bagi membolehkan pemadanan penuh di bawah sambungan kelajuan tinggi, platform NetFPGA digunakan sebagai prototaip dalam sistem ini. Hasilnya menunjukkan bahawa tandatangan yang dijanakan adalah sensitif dan tepat. Tambahan pula, suatu fungsi simulasi telah membuktikan bahawa rujukan suis NetFPGA adalah sesuai untuk membina padanan rentetan. Secara amnya objektif kajian ini diarkibkan dan sistem telah dibina dengan berjaya.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

ASCII	–	American Standard Code for Information Interchange
CAM	–	Content-addressable memory
CLB	–	Configurable Logic Block
CNET	–	Control version of NetFPGA board
COPP	–	COntent-based Payload Portioning
CPU	–	Central Processing Unit
DCAM	–	Dynamic Content Associative Memory
DMA	–	Direct Memory Access
DOS	–	Denial-Of-Service attack
FIFO	–	First In First Out
FPGA	–	Field Programmable Gate Array
FTP	–	File Transfer Protocol
HDL	–	Hardware Description Language
IDS	–	Intrusion Detection Systems
IO	–	Input / Output
IPS	–	Intrusion Prevention Systems
NIC	–	Network Interface Card
Pcap	–	packet capture
PCI	–	Peripheral Component Interconnect
PHP	–	Hypertext Preprocessor
RAM	–	Random-Access Memory
SOPC	–	System on a Programmable Chip
SSH	–	Secure Shell
TCP	–	Transmission Control Protocol
UART	–	User Datagram Protocol
UNET	–	User version of NetFPGA board
	–	

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

In the current days the utilization of internet are increasing rapidly. Many data and information are transferred through the internet every second. Additionally, the internet also became essential element in Human life (social, economic, educational even in his peaceful and security life), added to that, the internet is not immune, not safe and can be used to attack and harm the human life. For all these reasons the major challenge is how to prevent the network attacks and to secure information safetly. There are many security tools can be used to reduce the danger of internet, tools like Firewall, Defender walls, Antiviruses, IDS/IPS. Each one of these tools works in a different way and sometime one tool is not sufficient to protect a single machine or a small network. However, with the development of technology new and novel attacks appeared, to be able to defend we require advanced system. This system can be built with the help of other security tools and some hardware materials to speed up the system.

1.2 Problem statement

Larger bandwidths are widely used in the networking systems in these days, so it is becoming more difficult for traditional firewalls (especially the software firewalls) to function over a high-speed connection. In addition, current hardware firewalls are costly, difficult to run and setup, not updated automatically and have limited rules.

Current signature generators are not sensitive enough, they still produce high percentage of false positive signatures and true negative signatures [3, 2]. False positive signatures are dangerous because they cause a serious damage to the network if they

fail to identify the malware. The true negative signatures are signatures of a clean traffic but the generator classify it as malicious traffic which will slow down the process and reduce the system performance.

Firewall architecture implemented on NetFPGA in previous work is dependent, they can't function unless they connected to other resources like software firewalls or external devices [4]. Other firewalls slow down the network traffic, when a huge amount of signatures is present it will be very difficult for those firewalls to match the signatures with the coming traffic in a short time

1.3 Project objective

Objectives of this project is:

1. To generate malwares signatures from honeypot captured data using the Autograph approach. Honeypot samples will be used as dumpfiles which will be received be the Autograph to produce signatures.
2. To develop hardware architecture that able to scan moving data searching for signatures. The function of the architecture is to find similarity and alarm us.
3. To use a NetFPGA reference design to build the signatures matching hardware architecture. This architecture will behave as firewall.

1.4 Project scope

The limitation of this project:

1. The honeypot will be used to capture a copy of malware. This copy will be converted to Pcap format to be read by the Autograph. The Autograph output is a fixed size overlapped signatures.
2. Develop a simple HDL code to build a multi string matching architecture able to compare limited number (5 signatures in this project) of signatures with a sample of network traffic.

3. Integrate the string matching module into one of the NetFPGA reference designs to form the hardware firewall. Changes in the original code will be made if necessary, finally ensued that the new module is harmonious.

1.5 Report Outline

This report is organized into five chapters. The second chapter briefly explains the summaries of the literature review and list techniques, approaches and tools used to development the security systems also there are some reviews of previous work and related topics. Chapter three presents the basic concepts of the system and studies it's components along with followed methods to develop these components. Ultimate results of honeypot, autograph, string matching architecture and NetFPGA firewall are viewed in chapter four. Chapter five provides the overall achievement of this project. Suggestion for future work is included at the end of the chapter.

REFERENCES

1. Baumann, R. and Plattner, C. White Paper: Honeypots, 2002. URL `http://www.inf.ethz.ch/ plattner/pdf/whitepaper.pdf`.
2. Kim, H.-A. and Karp, B. Autograph: toward automated, distributed worm signature detection. In Proceedings of the 13th USENIX Security Symposium. 2004.1.10.
3. Yusof, M. B. Automated Signature Generation Of Network Attacks. Universiti Teknologi Malaysia. 2010.
4. M.S Chen, P. M. L. C., M.Y Liao and Yeh, C. E. *Using Netfpga To Offload Linux Netfilter Firewall.* Master's Thesis. 2010.
5. Gronland, V. A. *Building IDS signatures by means of a honeypot.* Master's Thesis. Norwegian Information Security Laboratory NISlab Department of Computer Science and Media Technology Gjovik University College. November 2009.
6. Spitzner, L. Honeypots Tracking Hackers. Pearson Education, Inc. 2003.
7. Forouzan, B. *Data Communications and Networking*. United State: McGraw-Hill Education (Asia). 2007.
8. Rajabi, H. *Behavioural Approach To Rapid Malcode Signature Generation.* Master's Thesis. Universiti Teknologi Malaysia. 2009.
9. Sarang Dharmapurikar, J. L. Fast and Scalable Pattern Matching for Network Intrusion Detection Systems. *IEEE journal on selected areas in communications*. 2006, vol. 24. ISSN 10. 1781 – 1792.
10. R.Kandhan, N. T. and Patel, J. M. Sigmatch: Fast And Scalable Multi-Pattern Matching. Computer Sciences Dn. 2010.
11. May 2011. URL `http://netfpga.org/`.
12. J.Naous, D.Erickson, G.A.Covington, G.Appenzeller, N.McKeown, Implementing an OpenFlow switch on the NetFPGA platform, In Symposium On Architecture for Networking and Communications Systems, 2008 (ANCS 08).
13. Monemi, A. NETFPGA tutorial. Universiti Teknologi Malaysia. August 2011.

14. MIT lincoln lab IDS corpus, 1999 DARPA Intrusion Detection Evaluation Data Set. [Online]. Available: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html.

15. Sourcefire. Snort, Online on May 2011. URL `http://www.snort.org`.

16. Cheng, J. *Silicon Firewall Prototype*. Master's Thesis. University of Saskatchewan. 2004.

17. Sourdis, I. *Efficient and High-Speed FPGA-based String Matching for Packet Inspection*. Master's Thesis. University Of Crete Electronic And Computer Engineering Department. July 2004.

18. Fisk, M. and Varghese, G. *An analysis of fast string matching applied to content-based forwarding and intrusion detection*. Master's Thesis. University of California. 2002.

19. Stanford-University. CPCI Architecture, Online on Jun 2012. URL `http://klamath.stanford.edu/NetFPGA/`.

20. Bu, L. and Chandy, J. A. FPGA based network intrusion detection using content addressable memories, April.

21. Virussign. Malware database, Online on Feb 2012. URL `http://www.virussign.com/downloads.html`.

22. F.M.M.Zain. *Machine Learning Approach To Malware Classifications/ Detection*. Master's Thesis.