IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-3 E-ISSN: 2347-2693

Modeling Multiple Packet Filter With FSA For Filtering Malicious Packet

Kakkad Kruti M* and Prof. Krunal Vaghela.,

Dept of Computer Engineering,
RK. University, Rajkot, Gujarat
www.ijcseonline.org

Received: Feb/24/2015 Revised: Mar/06/2015 Accepted: Mar/22/2015 Published: Mar/31/2015

***Abstract* -** In this paper we are trying to explain about firewall. Firewall is required to secure your valuable information. As there are many ways to deal with network security, we are trying to use FSA for providing a security because it is powerful enough to express any possible stateless packet filter and also provide optimal result in case of multiple packet filter combined together. As filtering is somewhat difficult with stateless packets we are trying to solve some issues related to stateless packet filter.

Index terms– Firewall, packet filtering, Stateful firewall, stateless firewall,FSA, WinPcap security policy.

I. INTRODUCTION

Computer network security is gaining popularityamong network users, with organizations investing more time and money to protect their valuable information. Security has also recently attracted considerable attentionfrom network researchers due to the importance of network security has grown tremendously. [1]

A **firewall** is a typical border control mechanism.A firewall is the front line defense mechanism against intruders.Firewalls can be **implemented** in both hardware and software, or a combination of both.**Stateful firewall** is a firewall that keeps track of the state of network connections travelling across it. Only packets matching a known connection-state will be allowed by the firewall; others will be rejected.

Stateless firewall is a firewall that treats each network Frame (or packet) in isolation. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

In computer programming, a filter is a program or section of code that is designed to examine each input and forward it accordingly.[2]

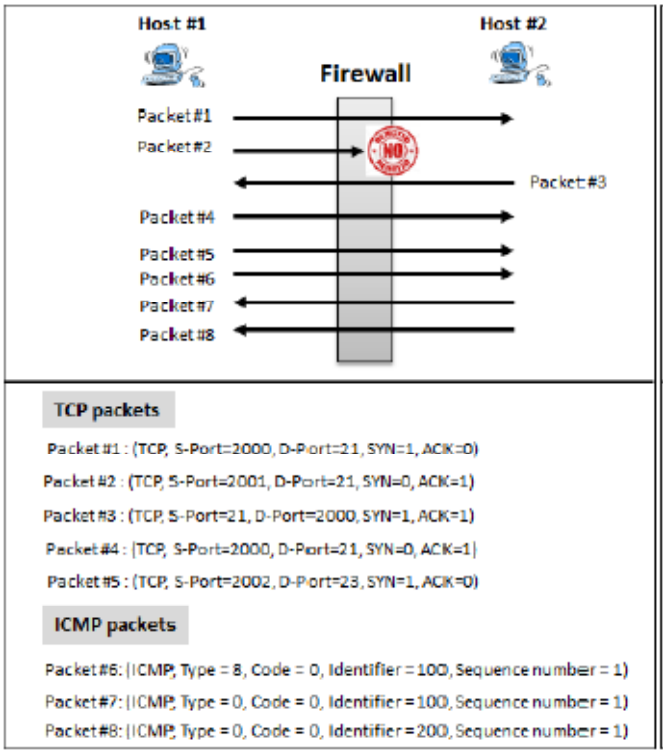

Figure 1 : List of packet accepted and denied by firewall

As shown in the figure 1 Host 1 and Host 2 are communicating through firewall, and transmitting the packets. Firewall will analyze the packet such as which protocol is user to communicate, and according to particular rule it will deny the packet to accept.

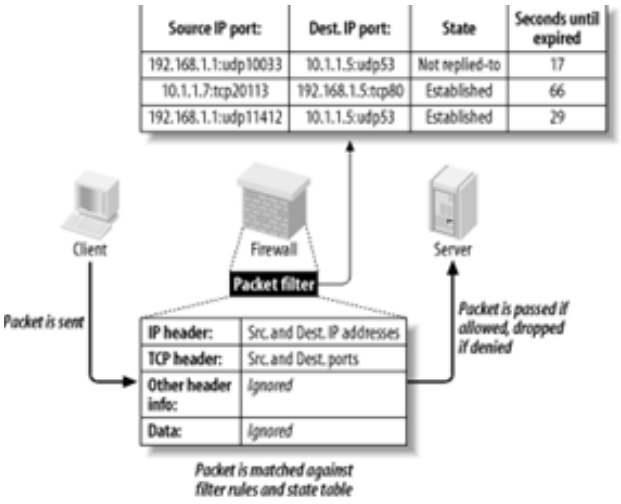

Figure 2 : Packet Filter

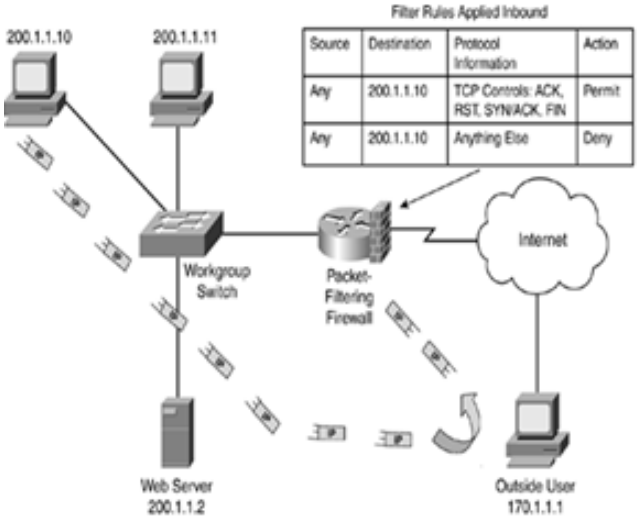

Figure 3 : Packet tracer

Figure 3 shows a packet tracer which trace the packet which are not from the current session or coming from the other port address and firewall will deny that packets.

II. Related Work

CMU/Stanford Packet Filter (CSPF) represents modern filter. It introduces the concept of Kernel level virtual machine. It executes the packet filter which can be defined at runtime. But its optimization capabilities are limited.[3]

Path Finder has the possibilities to compact control flow graphs for different packet filter. Each expression in filter is set in to the cells and each one describe the step in the construction of final check. Equivalent cell which are coming from the multiple filters are merged together. Filters are optimized only if they have a common prefix [4]

Berkeley Packet Filter (BPF) is also based on the virtual machine but it brings some notable improvements, such as it adopt the control flow graph model with helps to deploy compiler techniques to remove redundant checks from generated code. The BPF model is improved by BPF+ which uses more aggressive optimization. Which derived from software optimization techniques. And also it adds JIT compiler.[5]

Dynamic Packet Filter(DPF) [6] extends the approach of path finder. It introduces the capability to generate native code. Previously interpreter is used to run a filter.

Swift is used for packet filtering updates in a strict real time. Its ultimate goal is to add new filter immediately after three way hand shake is completed in tcp session. Which is done through the tree like structure. It enables multiple checks in parallel.[7]

III. Types of Packet Filtering

Packet filters act by inspecting the "packets" which are transferred between computers on the Internet. If a packet matches the packet filter's set of filtering rules, the packet filter will drop the packet or reject it. Each packet passing through is inspected and then the firewall decides to pass it or not. The packet filtering can be divided into two parts:

1. Stateless packet filtering.
2. Stateful packet filtering.

Stateless Packet Filteringallow/deny decisions are taken on packet by packet basis and these are not related to the previous allowed/denied packets then this type of filtering is called stateless packet filtering.Stateful Packet Filtering is if the firewall remember the information about the previouslypassed packets, then that type of filtering is Stateful packet filtering. These can be termed as smart firewalls. This type of filtering is also known as Dynamic packet filtering. [8]

IV. Tool WinPcap

WinPcap is a toolthat is used for capturing data packets in windows environments.

- This application allows the packets to transmit and bypass the protocol stack. This also has additional

futures like Kernel-level packet capturing and network statics engine to support remote packet capturing.

- WinPcap is used as the network interface by many tools, which are used for network packet scanning, network monitoring, traffic generators and network intrusion detection systems and so on.
- WinPcap as the core tool to monitor the network traffic. It can be integrated with many applications like Java, C# to analyze the packets.The tool is used for capturing raw 5data that is flowing in the network.
- WinPcap can also filters the data according to the rules that are created by the user.
- implementations of a lower level library for the listed operating systems, to communicate with those drivers [9]

V. FSA

Finite Automata or the state machine is a mathematical model to designing computer software and sequential logic circuits. FSA is used to model many important hardware and software applications. The various applications like the Network Intrusion Detection System(NIDS), Bio Informatics uses the Deterministic Finite Automata(DFA) for compiling large set of patterns. In the NIDS application, the patterns refers to the malicious attack patterns that harms the system or the entire network. In the Bioinformatics field, the DNA sequences are the patterns.The Network Intrusion Detection System aims at detecting the malicious network packets by inspecting the contents of the packet against the malicious patterns. A pattern is a group of characters that exist along with the malicious programs. Pattern matching is the process of matching the incoming packet contents with the known patterns of the malwares.

The security attacks are increasing day by day. Everyone is aware of the Twitter and Yahoo mail server attacks, numerous viruses, worms and Trojans are giving threats to the internet. To meet the high-speed requirements of current networks, many hardware architectures are proposed to accelerate pattern matching. Among hardware architectures, memory architectures have been widely adopted because of their flexibility and scalability.

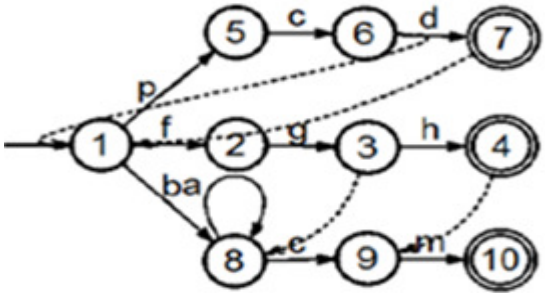

Figure 4 : A Finite Automata

There aretwo steps in designing memory architectures for pattern matching. The first step is to compile attack patterns into a deterministic finite automaton (DFA).Figure 4 shows three compiled patterns,"pcd", "fqh" and "bcm". 1 is the starting state and 7,4 and 10 are the ending states. The solid lines show the transition betweenthe states and the dotted lines shows the failure transitions. All the failure transitions are not given for simplicity.

Then the compiled DFA is converted into a state transition table and stored in the memory. The Figure 5 show the memory architecturein which state transition table is stored. Usually the memory will be the two dimensional memory, where each column represents the next state except the last one which indicates the Match Vector.

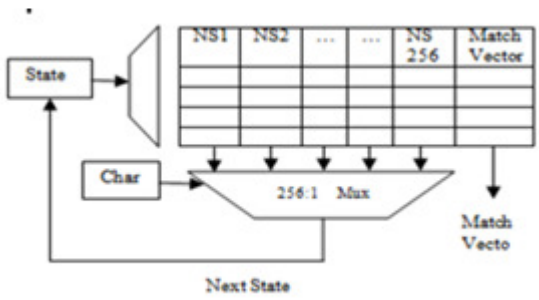

Figure 5 : basic Memory Architecture

The decoder converts the memory address to the corresponding memory location, which stores the next state and the matchvector information. When the input pattern arrives, the entire input pattern is matched against the pattern stored in the memory in the form of transition table. A "0" in the match vector which indicates that no "suspicious" patternis matched; otherwise thematched vector value indicates which pattern is matched.as the attacksare increasing day by day,we need to store large number of malicious patterns which requires more amount of memory. Hence most of the researchers are focusing on reducing the size of the DFA,to have a compact memory for storing the compiled patternsand also, to increase the searching speed. [10]

VI. CONCLUSION&FUTURE WORK

The FSA model is particularly valuable for this purpose because it is powerful enough to express any possible stateless packet filter. In FSA filters, each header field is examined at most once by construction; this property alone greatly limits the amount of redundancy in predicate

evaluation, a major source of inefficiency in packet filters. On the contrary, traditional optimization-based approaches cannot, by their own nature, provide any hard guarantee about the resulting code quality. FSAs also have straightforward and fast software and hardware implementations.

In existing system filter with FSA is introduced [11], In future we are trying to improve filter using FSA to improve the firewall.

References

[1]Meng-meng Zhang, Yan Sunand Jingzhong Wang,"A Fast Regular Expressions Matching Algorithm for NIDS", Applied Mathematics & Information SciencesanInternational Journal Mar. 2013

[2]Shubhash Wasti, Department of Computer Science, University of Saskatchewan, "Hardware Assisted Packet Filtering Firewall".

[3] J. C. Mogul, R. F. Rashid, and M. J. Accetta, "The packet filter: An efficient mechanism for user-level network code," in *Proc. 11th ACM Symp. Oper. Syst. Principles*, Austin, TX, USA, Nov. 1987, pp. 39–51.

[4]M. L. Bayley, B. Gopal, M. A. Pagels, and L. L. Peterson, "PATHFINDER: A pattern-based packet classifier," in *Proc. 1st USENIX Symp. Oper. Syst. Design Implement.*, Monterey, CA, USA,Nov. 1994, pp. 115–123.

[5] A. Begel, S. McCanne, and S. L. Graham, "BPF+: Exploiting global data-flow optimization in a generalized packet filter architecture," Comput. Commun. Rev., vol. 29, no. 4, pp. 123–134, Oct. 1999.

[6] D. R. Engler and M. F. Kaashoek, "DPF: Fast, flexible message demultiplexing using dynamic code generation," in *Proc. ACM SIGCOMM*, Stanford, CA, USA, Aug. 1996, pp. 53–59.

[7] Z. Wu, M. Xie, and H. Wang, "Swift: A fast dynamic packet filter," in *Proc. 5th USENIX Symp. Netw. Syst. Design Implement.*, San Francisco, CA, USA, Apr. 2008, pp. 279–292.

[8]Zouheir Trabelsi, UAE University, "Teaching Stateless And Statefull Firewall Packet Filtering: A Hands On Approach", 16th Colloquium for Information Systems Security Education Lake Buena Vista, Florida June 11 - 13, 2012.

[9] Navneet Kaur Dhillon and Mrs. Uzma Ansari,"Enterprise Network Traffic Monitoring,analysis and reporting using WINPCAP tool with JPCAP API",ijarcsse,Volume 2, Issue 11,November 2012.

[10]C. Jasmine, Dr. T. Latha,"Finite Automata in Pattern matching for Hardware based NIDS Applications – a Tutorial and Survey",Progress In Science in Engineering Research Journal,PISER 12, Vol.02, Issue: 02/06 March- April; Bimonthly International Journal Page(s) 351-360

[11]Pierluigi Rolando, Riccardo Sisto, Member, ACM, and Fulvio Risso," SPAF: Stateless FSA-Based Packet Filters", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 19, NO. 1, FEBRUARY 2011.

