Modelling Multiple Packet Filters with FSA for Filtering Malicious Packet

Kruti Kakkad
PG Scholar
Computer Engineering
RK University
Rajkot, Gujarat, India

Krunal Vaghela
Dy. Director
School of Computer Science
RK University
Rajkot, Gujarat, India

ABSTRACT
Computer network security is now a days gaining popularity among network users. Organizations are spending more time and money for securing their information. Security is also more considered by the network researchers due to the importance of network security has grown unbelievably. Finite Automata or the state machine is a mathematical model to designing computer software and sequential logic circuits. FSA uses pattern for filtering. 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 malware. In this paper we have tried to explain the firewall which improves the security with faster firewall mechanism. Our proposed solution provides filtering according to the keyword and port number. Also we have proposed new feature for the LAN users that is any user can interact with the other user of the same server. We have tried to propose a firewall which is dynamic where we can change the filtering rules. Previous work is limited when there is dynamic changes needed to the firewall. Also the important improvement is related to the time duration. Our proposed solution with FSA (Finite State Automata) regular expression takes less time for filtering of the packet compare to the algorithm which doesn't use the FSA.

Keywords
Firewall, packet filtering, Stateful firewall, stateless firewall, FSA

1. INTRODUCTION
Computer network security is now a days gaining popularity among network users. Organizations are spending more time and money for securing their information. Security is also more considered by the network researchers due to the importance of network security has grown unbelievably. [1][2]

A **firewall** is a typical border control mechanism. A firewall is the front line defense mechanism. Firewall can be implemented in both software and Hardware, or it can be combination of both of them. [3]

In computer programming, a filter is a program or part of code which is designed to examine each input packet and forward it accordingly. There are a number of packet filters currently available, both commercial and non-commercial. [2]

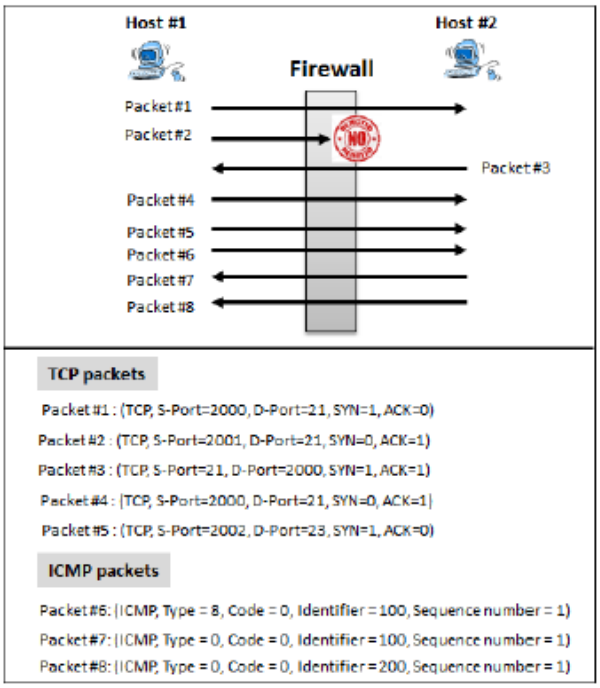

Figure1: List of packets accepted and denied by firewall

As shown in the figure 1, Host 1 and Host 2 are communicating through firewall, and transmitting the packets to each other. Firewall will analyze the packet such as which protocol is used to communicate, and according to a particular rule it will deny or accept the packet. As shown in the figure 1, packet 2 is denied. And other packets are allowed to communicate.

Also Figure 2 shows a simple firewall. This firewall is based on the port address. If port address of a packet is matched with the address contain by the table then packet is allowed and pass to the destination. If not allowed then it will drop the packet.

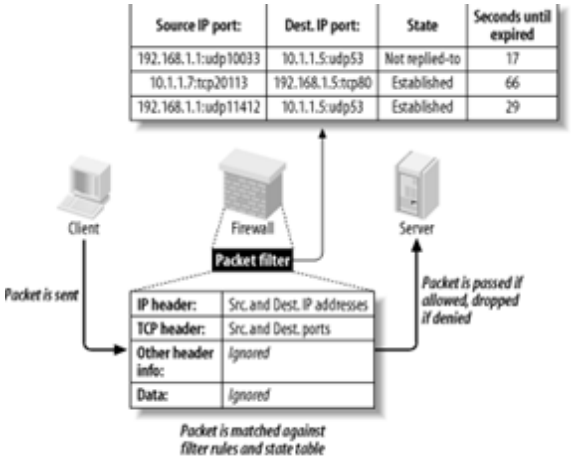

Figure2: Packet Filter

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. [4]

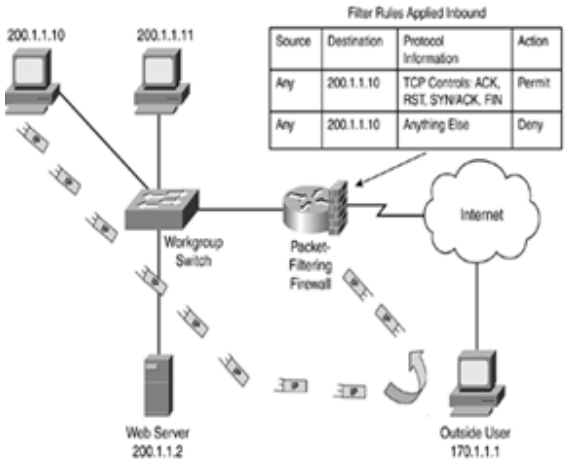

Figure3: Packet tracer

2. 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. [6]

Path Finder can compact control flow graphs for different packet filter. Each expression in filter is set in to the cells and each one of them describe the step in the construction of final check. All the cell which are coming from the multiple filters are merged together. Filters are optimized only if they have a common prefix [7]

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. [8]

Dynamic Packet Filter (DPF) extends the approach of path finder. It introduces the capability to generate native code. Previously interpreter is used to run a filter. [9]

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. [10]

3. TYPES OF PACKET FILTERING

Packet filters working as inspecting the packets which are transmitted between different nodes on the internet. If a packet matches with the filter's filtering rules, then it will allow the packet, otherwise the packet filter will drop 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 Filtering's allow/deny decisions are taken on packet by packet basis and these are not related with the previous packets which are allowed/denied. If the firewall remember the information about the previously passed packets, then this type of filtering is known as Stateful packet filtering. This type of filtering is also known as Dynamic packet filtering. [11]

4. 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. In figure 4 example of FSA is shown where 1 is starting state and 4,7 and 10 are final states.

As security attacks are increasing day by day. All are aware of the Twitter and Yahoo mail server attacks, numerous viruses, Trojans and worms are giving threats to the internet. Very high speed requirements of network is there, so to meet this many architectures are proposed, which are based on hardware. This is used to provide pattern matching faster. Among those hardware architectures, memory architectures have been widely accepted because of their flexibility and scalability [12].

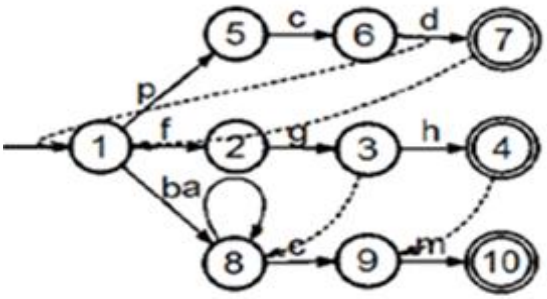

Figure4: A Finite Automata

5. PROPOSED WORK

We have proposed a scheme which will provide dynamic changes in filtering rules. Implementation is done using Java platform. Our proposed algorithm is less time consuming then other because of the FSA. FSA uses regular expression for pattern matching. If the pattern matches with the regular expression then it will block the site and deny the access for that particular user. Pattern matching is faster with FSA regular expression it will help algorithm to reduce the time. [4]. Interesting property is that each packet field is examined at least once when we are using it with FSA. [11] Our proposed scheme will allow user to specify own rule. So it will be more user friendly then other algorithms.

With this proposed work we have developed a filtering mechanism which is less time consuming because of string matching [14] and provide dynamic changes in filtering rules. Which is not possible with the previous solution. Also we will provide filtering with different parameters such as Port number and Keyword.

6. RESULTS ANALYSIS

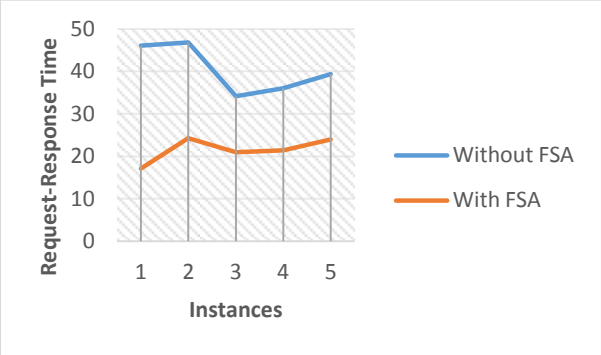

Figure 5. Comparison of Algorithm with FSA and without FSA in searching

We have proposed various techniques for filtering malicious packet. *First* technique is filtering according to the keyword. If there is some type of keyword used in user's URL which is not allowed by the program algorithm, then it will prompt the message that, that particular searched URL is blocked by the server.

Fig. 5 shows comparison for packet filter ratio of filtration program with FSA regular expression and without FSA regular expression. Comparison is taken based on the different instances. All the instance shows thee time difference between both With FSA and Without FSA algorithm. We can see that the packet filter ratio of program with FSA regular expression is apparently higher than that of without FSA program. Average request response time of packet filter with FSA is lower than without FSA because FSA uses pattern matching by regular expression which will match the pattern faster than matching the pattern as an integer.

Second technique is according to the port number. If we have blocked particular port number then user will not perform any action for example if server have blocked port no. 20 then user cannot perform any application related to FTP port.

As shown in figure 6 we have compare both the algorithm with FSA and without FSA regular expression for different port number. For example we have compare for port number 80 which will block the user to access any activity related to port http. As shown in the figure with FSA pattern matching algorithm it requires less time. Figure shows the improvement in result with respect to time in milliseconds. The reason behind this is FSA uses regular expression which match port number with the code faster.

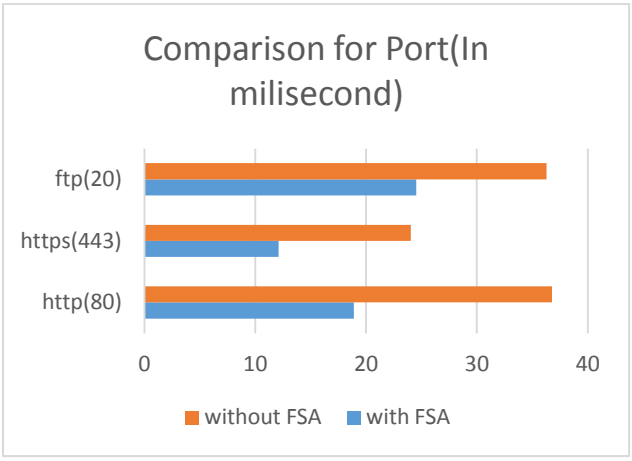

Figure 6. Comparison of Algorithm with FSA and without FSA with port

We have proposed chat as an extra feature in our proposed solution. Users which are logged-in from the same server can chat with each other when they are connected in LAN. For that while log-in user have to specify the person login name to whom they want to chat.

7. CONCLUSION AND FUTURE WORK

The FSA model is particularly valuable for the security because it is powerful for representing any possible stateless packet filter. In FSA every header is examined, at least one time. This property helps in limiting the amount of redundancy in evaluation of predicates, a major source of inefficiency in packet filters. In existing system filter with FSA is introduced. In this scheme implementation is done using Java platform. Our proposed algorithm is less time consuming then other because of the FSA. FSA uses regular expression for pattern matching. If the pattern matches with the regular expression then it will block the site and deny the access for that particular user. Pattern matching is faster with FSA regular expression it will help algorithm to reduce the time. Our proposed scheme will allow user to specify own rule

In future expansion the range of filtering with some other techniques may improve the result of filtering. Also more filtering can be proposed by which server can give more specific output.

8. REFERENCES

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

[2] Arti, Dr. S. S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks" \emph {International Journal of Advanced Research in Computer Science and Software Engineering}, Volume 3, Issue 5, May 2013 ISSN: 2277 128X.

[3] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim"Wireless Network Security: Vulnerabilities, Threats and Countermeasures "'International Journal of Multimedia and Ubiquitous Engineering"', Vol. 3, No. 3, July, 2008

[4] Marco Leogrande,FulvioRisso and Luigi Ciminiera,'"Modeling Complex Packet FiltersWith Finite State Automata"',IEEE/ACM TRANSACTIONS ON NETWORKING,1063-6692 , 2013 IEEE

[5] 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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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

[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

[12] 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

[13] 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.

[14] Jamuna Bhandari, '" Techniques Used in String Matching for Network Security"',International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:5, 2014.

[15] Marco Leogrande, Member, IEEE, Fulvio Risso, Member, IEEE, and Luigi Ciminiera, "Modeling Complex Packet Filters with Finite State", IEEE/ACM TRANSACTIONS ON NETWORKING · FEBRUARY 2015