A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities

Iman Kashefi*, Maryam Kassiri, Ali Shahidinejad*****

*(Faculty of Computing (FC), Universiti Teknologi Malaysia (UTM), 81300 Johor Bahru, Malaysia,)
**(Faculty of Computer Engineering, Robat Karim Branch, Islamic Azad University, Tehran, Iran,)
***(Faculty of Computing (FC), Universiti Teknologi Malaysia (UTM), 81300 Johor Bahru, Malaysia,)

ABSTRACT

Along with the increasing growth of computer networks, security threats multiplies and accordingly improving and enhancing the network security devices and methods become a necessity. Firewalls as the first line of defense have irrefutable importance in securing a network; therefore improvement in this technology ensures higher level of security in computer networks. Any improvement or novel ideas are not achieved unless a deep analysis of the existing methods and current needs takes place. In this paper the vulnerabilities of firewalls according to their natures and also various types of firewalls are classified in order to create a better perspective for future research. Also some of the current approaches to mitigate these vulnerabilities are mentioned and firewall fingerprinting as a technique which makes attackers able to obtain more precise information about firewalls` vulnerabilities in order to exploit them is presented.

Keywords – Firewalls, Firewall Fingerprinting, Firewalls vulnerabilities, Network Attacks, Network Security

I. INTRODUCTION

Firewall is one of the most powerful security guards that has been used widespread as a primary part of every network [1]. First it was assumed to exist between two networks; however, with the growth in use of internet and small size networks, it changed to one of the crucial aspect of every gateway to clog external intruder from accessing to LANs and any other private network. Since the firewalls are considered as the first and main line of defense in monitoring the inbound and outbound traffic in enterprise and backbone networks, the security and reliability issues are significantly important and should be carefully taken into consideration.

In spite of the fact that firewalls are considered as a useful defender in certain attacks, it comes with security holes that can be bypassed in some cases. Regarding the nature of computer and network devices, firewalls also have some limitations that can be misused by attackers [2]. For example a firewall can impede the intruders' access from outside the network, but it is not supposed to guard the network from an insider attack. On the other hand restraining inside attacks by access controlling has negative influence on user efficiency [3].

With respect to the crucial role of firewalls in network security, a systematic study on firewalls vulnerabilities is needed to further categorize the limitations with the purpose of helping researchers to gain a good perspective of problems in the first place to find practical solution to enhance the robustness of security.

This paper is divided into three sections; in the first section firewall and its types are described, the aim of the second section is to categorize firewall vulnerabilities according to their nature and various types and some of the current solutions to mitigate the vulnerabilities are presented, and finally the last section briefly describes firewall fingerprinting which can be used by attackers to identify type and characteristics of a firewall to misuse its vulnerabilities with the aim of launching a successful attack.

II. FIREWALL AND ITS TYPES

Firewalls have significant role in securing a network. For the purpose of protecting a network, firewall is used as the first line defense in almost every organization [4]. Firewall is considered as one of the efficient tools in providing top level of security in computer networks [5]. A firewall is a device or a system designed to block unpermitted access from inside or outside a private network. The greatest functionality of the firewall is filtering, in other words firewall has the responsibility of diverting the traffic with respect to pre-set policies, and by this means it can protect the system or network from flooding types of attacks [6]. As it is mentioned earlier, firewalls are used greatly for preventing unpermitted internet user from gaining access to a private network which is connected to the internet and this is achieved by filtering each incoming or outgoing packet to assure that both the source and destination of packets are trusted. Normally, firewalls configuration is in the way that protect network from unauthorized interactive login from outside. In this way "hackers" are prevented from logging into systems in a private network.

Firewalls are vital, regarding to the fact that they have ability to provide a block point where security is at risk. By constantly monitoring the traffic, firewalls can provide a safe auditing and logging, in most cases, they provide logs to the administrator about the type and volume of the network traffic. This block point does its job as an armed guard does. All incoming and outgoing data should pass through the firewall which control each single packet and obstruct those that are against the security criteria and pre-set rules. Firewalls rules are a set of predefined rules that each rule have an action and a related condition. The action is either deny or accept, while the related condition determines some information of the packets like the source and destination IP address, port number, protocol, and so forth. To maintain a decision regarding an individual packet, the rules are checked in turn till the first rule that its condition is met by the fields of the packet found. Generally the rule set is fully in detailed. When a firewall receives a packet, it checks out its protocol, the source and destination address and ports. Then the firewall compares the rules against the details of the packet until it finds a match. Different firewalls deployment applies various sequences of rules. Generally there are two matching strategies [7], single trigger and multi-trigger. Single trigger processing works in the way that as soon as it matches a rule, the action of it will be performed, while multi-trigger processing works in opposite way. In other words it performs the action of the last matching rule.

There are different ways to categorize types of firewall according to their architecture, functionality and their usage. Normally, from the user point of view firewalls can be divided into two types; hardware and software, but according to their architecture and functionality, a range from packet level to proxy firewalls can be defined, some of them are mentioned below [8]:

- Static Packet filtering firewalls: These kinds of firewalls sequence the packets concerning to allow/deny rules. It is done by the means of fields information on the header such as; host/ destination address or port numbers etc. this analysis is not in depths, i.e., malicious code detection is not performed and each packet is examined as a single entity. The primary weakness of these firewalls is the inability to sustain against fragment and spoofing attacks.
- Stateful packet filtering firewalls: These firewalls keep states of performance. Normally, in a client/server environment, client initiates a conversation with server and waits for server response. Accordingly responses are permitted to bypass the firewalls rules. In this way a better optimization in screening process is achieved that leads to empower the overall performance of firewall. In order to keep state tables, additional recourses such as memory with higher capacity are required.
- Stateful Inspection firewalls: These kinds of firewalls are the more advanced form of the stateful packet filtering firewalls. Stateful packet filtering firewalls are generally used for application that demand multiple ports, such as FTP applications. They check the payload and optionally open and close ports on the fly as per the protocol. This can be achieved through rules configuration and gain information concerning the fourth layer to the seventh layer of the protocol stack.
- Proxy firewalls: These firewalls isolate private network within internet. They evaluate the protocol syntax by breaking apart the connection between client and server. These kinds of firewalls offer a higher level of security among the other types of firewalls, but it is at the cost of functionality and speed, since they have the ability to limit the applications which your network can support. In contrary to stateful firewall that gives access or inhibits incoming or outgoing network packets in a protected network, traffic does not deluge through a proxy. Alternately, computers constitute a connection to the proxy that servers are intermediary devices, and commence a new network connection on the side of the request. In this way straight connections between systems on the both sides of the firewall are prevented, therefore it is not so easy for an intruder to explore where the network is, just because they can never receive packets straightly from the target system. The main disadvantage of this firewall is the need for huge network resources.

III. FIREWALL VULNERABLITIES AND THE MITIGATION THECHNIQUES

In this part the most important firewalls limitations and vulnerabilities are classified and existing proposed solution for mitigating them will be presented. “A firewall vulnerability is an error, weakness, or an invalid assumption made during firewall design, implementation, or configuration, that can be exploited to attack the trusted network the firewall is supposed to protect” [9]. According to this definition all the firewalls vulnerabilities can be classified in two main categories: (1) Vulnerabilities due to firewalls inherent limitations and design defects, (2) Vulnerabilities due to misconfiguration or weaknesses in implementation.

3.1 Vulnerabilities due to firewalls inherent limitations

Firewalls present an unreal illustration of security regarding to the fact that their inherent defects are constantly imposed to the hackers. These failings are caused by improper designs of the firewalls. Notwithstanding their helpfulness in providing security, they have some basic imperfections which hackers use to break into network. This problem causes inefficiency in guarding network.

Some of these limitations are common in both software and hardware firewalls while some are only found in software firewalls:

3.1.1 Common limitations in software and hardware firewalls

The most common vulnerabilities in software and hardware firewalls are mentioned below:

• Insider attacks: firewalls do not provide protection from insider threats i.e. Insider Attacks. It is acknowledged that insiders impose risks to security when they have limitless access to information, knowledge and valuable assets of their organization. They are granted access legitimately and this can easily jeopardize the security of the organization [10]. Firewalls sniff the packets in the boundaries of the networks and do nothing for the domestic traffic flow. Therefore, it is not practical for the intrusions which come from inside the network [8].

• Traffic that doesn't go through firewall: There are ways to route the illegitimate traffic through unpermitted path that does not pass through the firewall.

• Tunneling; Tunneling is one of the common methods applied to bypass the firewall; one can envelop message for a protocol inside some other message format [8].

• Internet threats like virus attack or password cracking: Firewalls do not carry out deep exploration to detect malicious codes in the packets; in this way they are likely to ignore some threats of this kind.

Below are some of the recommended solution and novel firewall models to alleviate above vulnerabilities:

Multipurpose firewalls: Intrusion detection systems have been used in order to audit whole activities inside a network but not as a specific mechanism against insider attacks. Disarming firewall proposed by Zubair A. Shaikh and Furqan Ahmed[11] is a multipurpose firewall which offers some defense mechanism against insiders. This firewall is a combination of various components; each of them presents distinct purpose. It bounds the attacking capabilities of all internal resources, in this way it can protect network against harmful insiders. Owing to the fact that gaining information from an end system is the first step for an attack, the firewall masks the identity of OS and server software which is positioned in DMZ from either internal or external users. The disarming firewall model takes advantage of the strengths of different methods to maintain the security. The significant strengths of this firewall are bounding the intrusion abilities of internal source, masking the identity of OS and server software in DMZ to obstruct attacks, and constantly observing and patching the software in the DMZ and intranet. This firewall model conquers a problem in traditional firewalls concerning VPN traffic. Portable users require access to organization data when they are out of office. Therefore they apply VPNs with the purpose of gaining access in a secure way. VPNs are not capable of guarding user's laptop or personal computer and these computers change into the potential places to threat the organization security because they are inherently two hosted to the organization's intranet and internet. They provide a security hole for an attacker. Traditional firewalls cannot do much to the traffic which is end-to-end encrypted [11]. The model is designed in the way that put the security in the focal point and the security is not overlooked for performance reasons. The firewall model is based on three concepts. First, most of the attacks have the inside source. Limiting the attacking abilities of individual host, leads to a secure internal network. In this way overall security is enhanced as disarmed internal host is not assumed as a threat to the rest of the internet. Second, attacks are implemented in the way that harms the network from the known vulnerabilities. These vulnerabilities are usually found in certain software's versions. In any types of attack, first the intruder tries to obtain the software's version to plan the attack in a way that imposes the published vulnerability. The information achieved by fingerprinting or social engineering is crucial for the success of an attack. Disguising the identity of the OS or server software will inhibit attackers to commence attacks. Third, security administrator may elude to install software patches due to various reasons such as unreliability, inaccuracy, irrevocability, and lack of enough knowledge. For this reason an automatic mechanism should be in place to install necessary updates as soon as they appear. By this means attacker have less chance to intrude to the network. And this is only practical with the emergence of networks that convey software patches [12].

Distributed firewalls: Another approach to alleviate the above mentioned vulnerabilities is applying distributed firewalls.

Distributed firewalls have been designed with the purpose of providing higher level protection than traditional firewalls such as gateway and host-based firewalls. Distributed firewalls have been developed in response to the need of securing network from insider attacks and of course cover the weakness of either gateway or host-based firewalls. According to Ioannidis et al. [13], "a distributed firewall is a mechanism that enforces a centralized security policy but the latter is applied at the edges". Distributed firewalls are designed in the way that regulates software applications which are resided in host that have the responsibility of protecting a network against unauthorized access. The notional design of distributed firewalls are based on three elements [14]: First, A common place policy language which is employed for determining security policies which are distributed to the firewall endpoints to configure distributed firewalls. Second, Network-wide mechanisms for the distribution and application of the security policy files to the distributed firewall endpoints. Third, IPsec: security protocol that maintain network-level encryption for the secure transmission of the security policy. Distributed firewalls have following strengths:

•Centralized management: Security policies are planned centrally and then publish to the various endpoints for execution. Adherence of security policies through the network and managing the deployment is improved.

•Defense in depth: when distributed firewall is used with the gateways firewall, the security layers are notably increased which makes it more difficult for an intruder to break into the network. Because it saves the time for other kind of defense mechanisms to counteract the hazard dramatically and accordingly delay and prevent the distribution of threat in the network.

Distributed firewalls also have their own limitations like decrease in network performance and increase in host load. Therefore in order to mitigate these disadvantages several architectures and models have been introduced and still should be improved.

Combining firewall and IDS: There are two approaches to combine firewalls and IDS: integrated approach and linkage approach. In first approach both IDS and firewall are placed in one system while in second approach they are in two separate subsystems [15].

• Integrated Approach: The integrated approach benefits from the advantages of the revelation ability of the detection system along with the blocking capability of the firewall. In this approach the host IDS and host firewall are placed in the same system. Since the IDS is constantly monitoring the network, it provides the access control strategy source to the host firewall. In this way malicious requests are detected before the attack occurs [16]. In this approach traditional access control is combined with intrusion detection technology to supply essential information to enable the firewall to block attacks.

• In this method, the host firewall is located in a one system while the host intrusion detection system is running on a separate system. The hosts interact in a meaningful manner to share the information to enhance the security level to maximum possible degree. This method differentiates from integrated method in the location of the IDS and the firewall. This approach has dual implementations. In the first deployment the host firewall is directly linked to host IDS, while in the second deployment, a transfer device is employed to link the two hosts indirectly [17]. In both deployments unified communication interface is needed. It is proved that linkage method takes advantage of independency, high reliability, and less response time in contrary to the integrated approach.

3.1.2 Vulnerabilities in software firewalls

Nowadays software firewalls are the most popular choice for installing on personal computers. They use internet access control mechanism to provide higher level of security for internet users. These kinds of firewalls have vulnerabilities that can be bypassed in various ways at different layers of networks. This is essentially due to the fact that these kinds of firewalls are software. They are not designed based on a proper architecture; therefore they allow some traffic and application to pass through them. Below are some of the theoretical bypassing ways [18].

• NIC Adapter Driver: An easiest way to bypass any kind of software firewall is to plan the program in the way that runs in a lower level. Regarding to the fact that the commercial personal firewall execute at NDIS level while NDIS is located between NIC and protocol driver, therefore if the program runs at NIC level, it can bypass the firewall. However, it is not practical since the Trojan code which is programmed for a specific NIC will not be able to run on the others.

• Prevent Loading: Since these firewalls occasionally store data in the registry, if the registry is manipulated, it may be feasible to obstruct some firewalls from running after restarting the system.

• Uninstall: Another way to bypass a personal firewall is by simply uninstalling theme. There are many hacking codes which are particularly designed to uninstall famous firewalls.

• Application Masquerade: Generally the firewalls do not obstruct all the traffic. Some applications are permitted for getting access to the internet. Sometimes hackers program a malicious code in the way that it seems like a trusted program, so it can simply bypass the firewall.

• Application Control: Sometimes a program employs a trusted application to send and get unauthorized messages to outside, should the program be able to manage the way the programs uses to perform its actions.

• Network-monitoring programs: Approximately network-monitoring programs are overlooked by personal firewall. It is obvious that if a malicious program can work like one of the network monitoring software, it will be able to bypass personal firewall.

It can be concluded from the above that personal firewalls are defenseless to many intrusions. To improve the level of protection of personal firewall to a higher degree, it is recommended to use it along with constantly up-todate antivirus software. Concurrently, it can be a potential field for research to fortify the protection level of personal firewalls from hardware perspective.

3.2 Vulnerabilities due to misconfiguration

While the part of vulnerabilities which come from misconfigurations are the result of weakness and complexity of firewalls design and user interfaces, there are notable reasons which concerning user faults and their incapability of implementing and managing different aspects of firewalls. Carelessness and misuse can be the biggest threat to any security system anywhere [19].

It is worth mentioning that improper use of security system can be more detrimental than relinquish the use of them. The false illustration of security that inspired by a misconfigured firewall makes users behave like they are fully secured, while they are treated with the same risks. Personal firewall are imposed more to misconfiguration, since the knowledge for implementing firewall in the safe manner may go beyond the capability of common users.

The following are the common vulnerabilities associated with misconfigurations of the firewalls [9]:

- ICMP allowed, e.g., the firewall can be pinged;
- Denial rather than drop the traffic to ports which are blocked by the firewall. This provides the attacker with additional information, or improves the speed of the attacker's port scan;
- Misconfiguration that allows a TCP pings of internal hosts with Internet-routable IP addresses (e.g., in-bound TCP 80 is not restricted to the web server)
- Trust of certain IP addresses
- Availability of extra/unnecessary services on the firewall
- Unnecessarily open TCP and UDP ports

As mentioned before a part of misconfigurations are related to some other important issues such as configuring inattentively. For instance when the program needs to be configured, occasionally it may happen that the users are tired of responding to many questions and perfunctorily switch off the security warnings. These kinds of problems take place because of poor usability in personal firewalls. Poor usability of a security system can have severe aftereffects as are mentioned in several articles. According to Bander Alfayyadh et al. [19], usability of personal firewalls is especially important and interesting to study because most of the personal firewall users have little information about security issues. They have shown that the main problems arose in personal computer are due to the poor usability that accordingly result in security vulnerabilities. It is worth pointing out that the primary concerns of firewall designers are security robustness rather than great usability. Nevertheless more the usability improved, the better results achieved. There is fine balance between usability and security that it only realized by comprehensive design which includes usability in development phases. There are many usability best practices for security design which can be taken into account. It is possible to classify the usability issues in two main classes. First there is ambiguity in information or sometimes lack of knowledge when the users should make decision on security issues. Second, poor user interfaces which result in security alerts ignorance. As a solution to this problem, firewall designer can fortify the quality of information through the results from usability testing with end users. Moreover, it can be a good practice to involve usability experts in design process.

IV. FIREWALL FINGERPRINTING

Vulnerabilities mentioned in the previous section both in hardware and software firewalls along with other vulnerabilities caused by flaws and shortcomings that may exist in some specific models of different firewall brands are more probable to be exploited by attackers if they can acquire enough information about the employed firewall in a computer network.

Regarding to the fact that firewalls are usually positioned in a network so that they are invisible to the users, the identification of them to explode their vulnerabilities to do a successful attack is dramatically complicated. To launch a successful attack, the first step that the attacker should take is fingerprinting, *i.e.*, finding the firewall implementation, encompassing the brand name, software/firmware version, etc. Providing that we figure out all possible ways that attackers employ to fingerprint a firewall, we will be able to design required countermeasures accordingly.

A recent research conducted by Amir R. Khakpour et al. presents a set of techniques that acquire some basic information about firewalls using the processing time of each inquiry packet and can be employed to find firewall implementation. By precisely measuring packet processing time, it is possible to fingerprint firewalls to figure out the type of packet classification algorithms, sensitivity of firewall performance to traffic load, and other characteristics. They proposed some ways to identify the firewall characteristics that are announced by firewall implementations. Even though the firewall is designed like a black box, attackers can misuse vulnerabilities of these kinds of firewalls from their characteristics that are precisely identified to launch effective attacks. They presented two methods for deducting firewall implementation using these characteristics. The first method is concerned with firewall decision while receiving a sequence of TCP packets that carry unusual flags; the second method is based on machine learning techniques [20]. By using these methods they could acquire relatively accurate data about the firewalls and could successfully fingerprint the three different types of firewalls, both software and hardware, which they had used for this project.

The results of their work show that firewall fingerprinting can become a serious issue that causes exposure of firewall vulnerabilities and should be taken into consideration simultaneously along with making effort to mitigate firewalls vulnerabilities.

V. CONCLUSION

The classification of firewall vulnerabilities which is presented in this paper along with the mentioned existing solutions can be a helpful guideline for researchers who aim to enhance the security of firewalls and also can give them a clear and precise perspective of existing problems in this field.

Integrating the capabilities of firewalls and IDS and also fortifying the protection level of personal firewalls from hardware perspective still can be potential fields for future researches. Regarding this study on existing types of vulnerabilities and also defense models in firewalls, a unified model which takes benefit from the strength points of different solutions and accordingly mitigate the vulnerabilities of the models to maximize the robustness of security and protection capability of network may be a good solution. Although integrating various models in a system may cause some conflicts and have inverse effects, still there would be a potential area for further research to propose an integrated model that brings more security. Moreover, not only practical solutions to improve the security in firewalls through mitigating their vulnerabilities should be carefully followed, but also in the meanwhile, conducting a research for finding countermeasures to prevent firewalls from being fingerprinted by attackers should be taken into consideration, since firewall fingerprinting increases the probability of exposure of vulnerabilities to the security attacks.

REFERENCES

[1] R. Bace, An Introduction to Intrusion Detection and Assessment for System and network security Management, ICSA, Inc http://www.icsalabs.com/icsa/docs/html/communities/ids/whitepaper/Intrusion1.pdf.

[2] Cisco Firewall Services Module DoS vulnerability, http://www.netsecurity.org/secworld.php?id=10673, 2011.

[3] J. Craig Lowery , Computer System Security: A Primer, March 2002, http://www.craiglowery.com/pres/Computer%20System%20Security-%20A%20Primer.pdf

[4] W. Geng, S. Flinn, and J. DcDeourek, Usable firewall configuration, Proc. 3rd *Annual Conference on Privacy, Security and Trust*, Institute of information technology, national research council Canada, 2005.

[5] Ghiran, A.M., Silaghi, G.C., and Tomai N., Ontology based tools for automating integration and validation of firewall rules, *Proc. of 12th international conference on Business Information Systems*, Poland, 2009, 37-48.

[6] V.M. Boncheva, A Short Survey of Intrusion Detection Systems, Problems of Engineering Cybernetics and Robotics, 58, 2007.

[7] V. Zaliva, Firewall Policy Modeling, Analysis and Simulation: a Survey , 2010.

[8] S. Beg, U. Naru, M. Ashraf, and S. Mohsin, Feasibility of Intrusion Detection System with High Performance Computing: A Survey, IJACS, December 2010 .

[9] S. Kamara, S. Fahmy, E. Schultz, F. Kerschbaum, and M. Frantzen, Analysis of Vulnerabilities in Internet Firewalls, CERIAS.

[10] C. Colwill, Human factors in information security: The insider threat - Who can you trust these days?, Information Security Technical Report. 2010, 14(4), 186-196.

[11] Z. A. Shaikh and F. Ahmed, Disarming Firewall, *Proc. International Conference on Information and Emerging Technologies*, ICIET, 2010.

[12] J. Li, P. L. Reiher, and G. J. Popek. Resilient Self-Organizing Overlay Networks for Security Update Delivery. IEEE Journal on Selected Areas in Communications (JSAC), January 2004

[13] S. loannidis, A. D. Keromytis, S. M. Bellovin, and 1. M. Smith, Implementing a distributed firewall, *Proc. 7th ACM Conj. Computer and communications security*, Athens, 2000.

[14] V. Ramsurrun and K. M. S. Soyjaudah, A Stateful CSG-based Distributed Firewall Architecture for Robust Distributed Security, UoM.

[15] Zh. Lili and C. Tian-jie. Intrusion Detection Based on Intelligence and Collaboration Technology Computer, 2008, 24 (2): 66-68.

[16] Zh. Tao-gai and L. Ke, A New Design of Linkage Based on IDS, Henan Institute of Engineering (Natural Science), Vol • 21, No • 3 Sep. 2009.

[17] Zh. Zhong-hui and C. Jia-qing, Intrusion Prevention System Based on Linkage Mechanism Computer age, 2006, (7) :28-29

[18] R. Chiong and S. Dhakal, On the Insecurity of Personal Firewall , IEEE, 2008.

[19] B. Alfayyadh, A. Jøsang, M. Alzomai and J. Ponting, Vulnerabilities in Personal Firewalls Caused by Poor Security Usability , IEEE, 2010

[20] A. R. Khakpour et al. , “Firewall Fingerprinting”, 2012 Proceeding IEEE INFOCAM, 2012