International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 85-94 | Cosmos Impact Factor (Germany): 5.195
Received: 02.02.2018 Published : 28.02.2018

DESIGN OF EMBEDDED WEB SERVER USING ARM S3C2440 TO PREVENT ONLINE ATTACKS.

Kuttimani, S.Pratiba
Department of Electronics and Communication Engineering
Dhanalakshmi Srinivasan Institute of Technology, Samayapuram, Tamil Nadu, India

Abstract

Denial of service attacks prevents legitimate users from using a service. One particular type of this attack is known as SYN flood, where external hosts attempt to overwhelm the server machine by sending a constant stream of TCP connection request. There are several approaches for dealing with this attack that firewall is one of them. In this paper we attempt to prevent this type of attacks with iptables firewalls. Any Firewall prevents unauthorized use and access to your device, its job is to carefully analyze data entering and exiting the device based on user configurations and ignore information that comes from suspicious locations. The firewalls available in the market are general purpose and not suitable to the Embedded boards. Hence I developed and implemented a firewall for an ARM9 processor which uses Linux as the operating system. The Firewall design used Net filters concept in Linux for an ARM9 processor. After implementing the firewall, experimentation was done to study the extent to which the firewall can prevent the securing attacks especially SYN flood attack. Packet filtering concept is used to examine the header of a packet to determine the source and the destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped. Hence it is established in this paper by implementing the firewall based on Iptables rules one can avoid SYN flood attacks from ARM Board.

Keywords— SYN flood Attack, Iptables, Firewall, Friendly ARM.

I. Introduction

The firewall prevents unauthorized use and access to the specified device, its job is to carefully analyze the data entering and exiting the device based on user configurations and ignore information that comes from a suspicious location. Generally, attacks are the techniques that the attacker uses to exploit the vulnerabilities in applications. Most of the attacks are Denial of Services attacks (DoS). DoS attack prevents legitimate users from using a service. One particular type of attack is known as SYN flood attack, where external hosts attempt to overwhelm the server machine by sending a constant stream of TCP connection requests. There are several approaches for dealing with this attack that firewall is one of them. In this paper, we attempt to prevent of this attack with iptables firewalls.

Iptables firewall is a Linux oriented firewall. Iptables is a software and stateful firewall that monitor on the header of packets and filters packet. At the beginning of this, we describe some of the computer's attacks known as Denial of Service attacks and explain one of them, in the name of SYN flood attack. The next section details involved firewall definition, its types and iptables firewall. The firewalls available in the market are general purpose and not suitable to the embedded boards, hence we can develop and implement a firewall for an ARM processor which uses Linux as Operating system. The Firewall is developed by using Net filters / Iptables concept in Linux for an ARM processor. In the next section, we familiar with firewall structure and describe firewall rules components and learn how we can build its rules. In the next section, we talk about the state of a packet and porting rules into ARM Board. In the last section of this project described how to prevent of SYN flood attack with iptables firewall and show the rules that used for this goal.

II. Denial Of Service Attacks

Generally Attacks are the techniques that the attacker uses to exploit the vulnerabilities in applications. Most of the computer attacks are Denial of Service (DOS) attacks. The Denial of Service attack is attempted to make a computer resource unavailable to its intended user. A denial of service attack may target a user, to prevent them from making outgoing connections on the network. It may also target an entire organization, to either prevent outgoing traffic or to prevent incoming traffic to certain network services, such as the organizations' web page [1].

Denial of service attacks is much easier to accomplish than remotely gaining administrative access to a target system. Because of this denial of service attacks have become very common on the Internet. DOS attack has different types that the earliest form of them is the flood attack. The attacker simply sends more traffic than the victim could handle. This requires the attacker to have a faster network connection than the victim. One of the most famous forms of flood attack is SYN flood attack. When the session is initiated between the Transfer Control Protocol (TCP) client and server in a network, a very small buffer space exist to handle the usually rapid "hand shaking" exchange of messages that sets up the session. The session establishing packets include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This leaves the first packet can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these bogus connection requests is to make it difficult for legitimate requests for a session to get established. In general, this problem depends on the operating system providing correct settings or allowing the network administrator to tune the size of the buffer and the timeout period [2].

Hping3 is a network tool, it supports to generate this type of attack. Hping3 is a command-line oriented TCP/IP packet crafter. It can be used to create IP packets containing TCP, UDP or ICMP payloads. All header fields can be modified and controlled using the command line. Hping3 is also called as a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping (3) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. While Hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts.

A subset of the stuff you can do using hping.

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting

Hping is quite an easy and fast utility to check firewalls spoofing rules. Simply create a spoofed packet with the switch and target them against machines in the DMZ/INTERNAL LAN, and check if the firewall actually drops the illegal packets. Hping is DoS tool. My point is the following section is not proof that I can create a denial of service conditions, but it is an easy way the audit IDS and firewall setups. To avoid sending a TCP reset packet from the attacking machine, use a spoofed IP address with a switch. If you want to increase the pps rate, use the switch to indicate the interval (ex: i u1000, means every 1000 microseconds). Ex:- hping -I eth0 -a 192.168.10.99 -S 192.168.10.33 -p 80 -i u1000 Hping is a very useful utility when learning TCP/IP and actually understand what happen. People auditing firewalls /IDS system can find great benefits in using hping. Various depending mechanism exists for preventing of this attack that can among them point to firewalls.

III. Firewall

A firewall is a software of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a command or set of commands configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

A firewall is a dedicated appliance, or software running on a computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules [1].

Firewalls can be implemented in either hardware or software or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the internet, especially intranet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Firewalls make it possible to filter incoming and outgoing traffic that flows through your system. A firewall can use one or more sets of “rules” to inspect the network packets as they come in or go out of your network connections and either allows the traffic through or blocks it. Firewalls mainly divided into two categories.

Stateless firewalls: Stateless firewalls watch network traffic, and restrict or block packets based on source and destination addresses or other static values. A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall ‘pretending’ to be something you asked for.

Statefull firewall: Statefull firewalls maintain context about active sessions, and used that “state information” to speed packet processing it maintains records of all connections passing through the firewall and is able to determine whether a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.

IV. Netfilter Framework

The Netfilter in the Linux kernel is able to keep track of the network packet’s state and context. This means that Netfilter can distinguish packets associated with an established connection from packets that are not. For example, if you connect to a web server with your browser, the webserver answers your browser’s request and Netfilter knows that these incoming network packets are the response to the request you initiated with your browser. Using this feature allows you to instruct Netfilter to only accept network packets that are part of an established or related connection initiated by you but to ignore all other network packets.

- NEW: The packet is trying to start a new connection.

- ESTABLISHED: A connection that has seen packets travel in both directions.

- RELATED: A packet that is starting a new connection but is related to an existing connection.

- INVALID: This packet is associated with no known connection. These packets should be dropped.

A normal example would be that the first packet the contact subsystem sees will be classified “new”, the reply would be classified “established” and an ICMP error would be “related”. An ICMP error packet which did not match any known connection would be “invalid”.

Netfilter is a framework that provides hook handling within the Linux kernel for intercepting and manipulating network packets. It can filter the packets at different levels. There are five Routing levels, they are

- Pre Routing
- Input
- Forward
- Output
- Post Routing

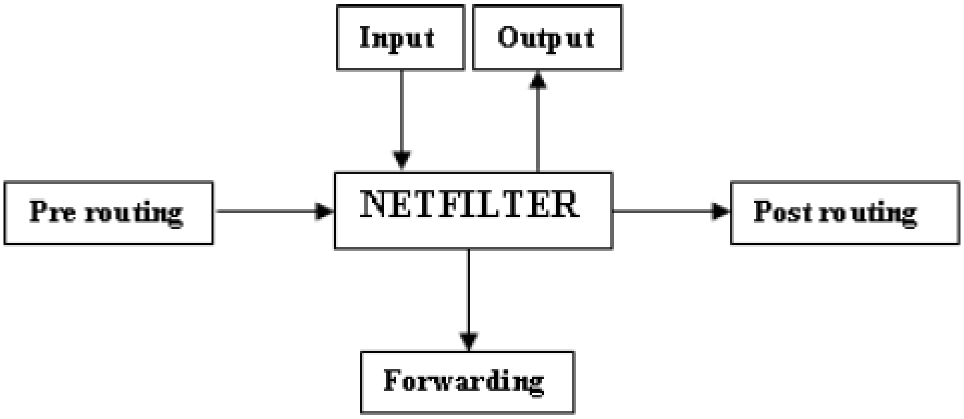


Fig.2. Net Filter Block Diagram

At these routing levels, the packet filtering will occur and the actions occurred [4].
1. PREROUTING - For altering incoming packets before routing.
2. INPUT - For Packets destined to Local Sockets.
3. OUTPUT - For altering locally-generated packets before routing.
4. FORWARD - For altering packets being routed through the box.
5. POSTROUTING - For altering packets as they are about to go out.
There are four types of actions that can perform on these different routing levels and the actions are
1. ACCEPT - This means to let the Packet accept.
2. DROP - means to drop the packet.
3. QUEUE - means to pass the packet to userspace.
4. RETURN - means stop traversing chain and resume the next rule.

V. Embedded Arm Processor

ARM is a 32-bit Reduced Instruction Set Computer (RISC). It is known as the Advanced RISC Machine, and before that as the Acorn RISC Machine. The relative simplicity of ARM processors makes them suitable for low power applications. As a result, they have become dominant in the mobile and embedded electronics market, as relatively low cost, small microprocessors, and microcontrollers. In 2005, about 98% of the more than one billion mobile phones sold each year used at least one ARM processor. As of 2009, ARM processors account for approximately 90% of all embedded 32-bit RISC processors and are used extensively in consumer electronics, including PDAs, mobile phones, digital media, and music players, hand-held game consoles, calculators and computer peripherals such as hard drives and routers. Prominent examples of ARM Holdings ARM processor families include the ARM7, ARM9, etc. The ARM architecture has the best MIPS to Watts ratio in the industry, the smallest CPU die size. ARM processor features include Load/store architecture, an orthogonal instruction set, mostly single-cycle execution, a 6x32-bit register, enhanced power-saving design. The small size, low cost, and low power usage lead to one of the most common uses for an ARM processor today, embedded applications. Embedded environments like cell phones or PDAs (Personal Digital Assistants) require those benefits that this architecture provides.

Nowadays embedded ARM boards are available readily in markets like Friendly ARM Products. It is an embedded product with ARM9 processor. It has more built-in features like,

- It is Linux-ready, hardware/software development kit for Samsung's ARM9-based S3C2440 microprocessor.

- The S3C2440 system-on-chip (SoC) primarily targets handheld devices such as smartphones and PDAs. The SoC integrates 16KB each of instruction and data cache, 4KB RAM, a NAND flash boot loader, power management functions, an interrupt controller, and an external memory controller.

- The Mini2440 comes standard with 256MB each of SDRAM and NAND flash, expandable via an SD card slot, along with 2MB of NOR flash. The board has camera and LCD interfaces and with a built-in 3.5-inch QVGA (320x240) TFT Touch Screen LCD.

- The Mini2440's complement of PC-style I/O includes Ethernet, USB host, and slave ports, and three serial connections. Available options include a WiFi module, and CMOS and USB camera options. The Mini2440 board offers a "stable CPU power source chip and reset the system.

The MINI2440 is a single board computer based on the Samsung S3C2440 microprocessor. It is a Friendly ARM [5].

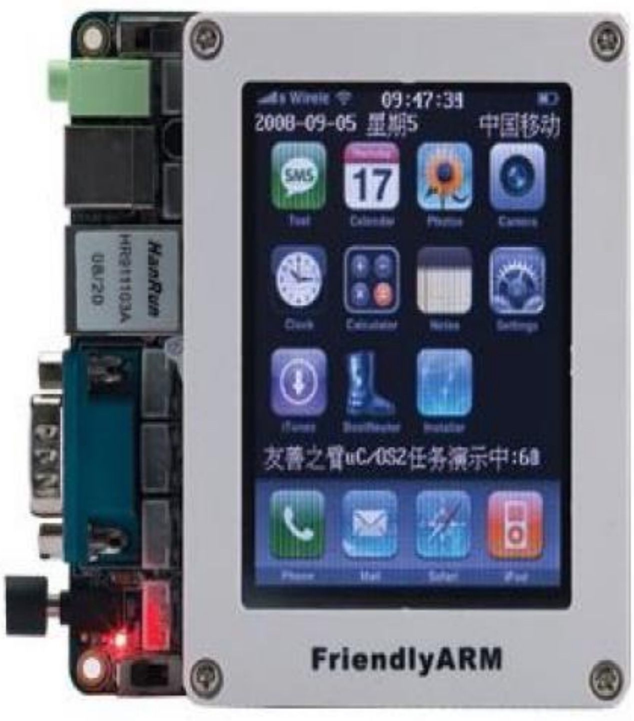


Fig.3.An Overview of ARM 9 Samsung S3C2440 Kit

VI. Implementation Model

One of the simple strategies taken to prevent of DOS attack is to limit the number of connections and the packet delivered in time. Since it is a state full firewall, iptables has the number of packets sent through a connection. Any user can send specific number of SYN packet within certain intervals, however, they are dropped if they will exceed.

Firewall extensions such as recent, fuzzy and limit are used to apply the limit. Thus the attack is prevented.

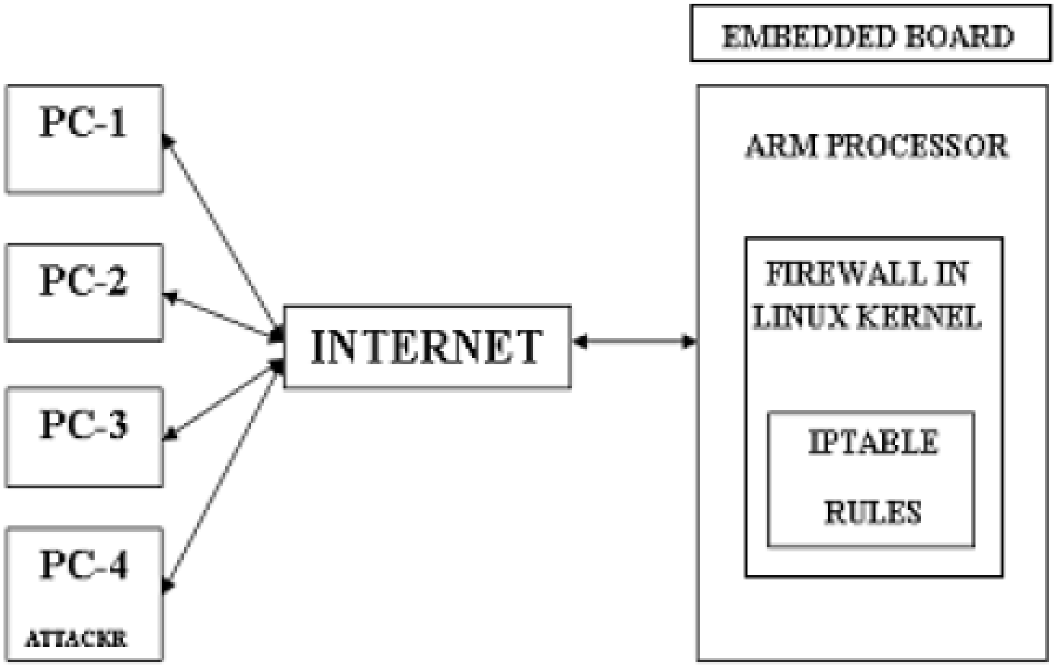
1) Motivation

In the present scenario where ARM processor is extensively used in consumer electronics like PDAs, mobile phones and routers, include Internet access. Access to the Internet involves the risk of exposing sensitive data, securing these increasingly popular devices comes as a challenge. So, we have to provide security for these sensitive data.

2) Objective

The main objective of this project is to provide security to embedded boards. Hence we are implementing our own firewall on an ARM processor that can provide a basic level of security to embedded boards.

3) General Scenario



Block Diagram

ARM processor is capable of running open-source operating system Linux thereby providing facilities such as multi-tasking environments, designs that include networking.

Hence Linux operating system is porting into the ARM processor. And also we are adding some rules into ARM processor. These rules are defined with the help of Iptables. Hence making new rules using Iptables is called a firewall. These iptables and rules are porting into the Linux kernel on ARM board.

The packets are sending and receiving through TCP handshaking model. TCP handshaking is also called as Threeway handshaking because the client will send SYN-REQ to the server and the server again will send SYN-ACK if he is ready to access. The client responds with an ACK, and then a connection is established.

PC1, PC2, PC3, and PC4 (attacker) are the different users to access the ARM board through the internet. PC1, PC2, and PC3 are responses with ACK back to the server. So the connection is established i.e., packets are sending and receiving between clients and servers. But PC4 is sending continuous TCP requests without sending back to ACK to server. Hence it is an SYN flood attack. According to Iptables rules ported into to kernel on ARM board, the server will drop these packets and continue authorized client's packets.

According to the general scenario, if the attacker will send continuous requests i.e. SYN flood attack to ARM board through the net, then the firewall will detect the attacks and prevent that attack from the attacker.

VII Results and Conclusion

1. If SYN flood attack has occurred on ARM board, then ARM web server is not opened.

2. After ported Iptables rules into the ARM board, if the attacker will send attacks to ARM board, but it can open web server because Iptables firewall is present on ARM board. So this is the prevention of SYN flood attack.

Packets are filtered by iptables firewall using Netfilters and basic security is been achieved by the firewall. Linux kernel provides a mechanism to implement our own firewall. This mechanism is called "Netfilters". Hence Packet filtering using Netfilters can successfully be implemented on an ARM processor. The Linux Kernel [6] is configured to monitor the incoming and outgoing packets. Packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. If the packet does not match a rule the packet is dropped. Highly sensitive devices can be protected, as the firewall is developed.

The firewall developed is free of cost and also provides a basic level of security. Netfilters firewalls can drop packets based on protocols like HTTP, ICMP and based on source and destination IP address. Hence the user can configure and derive many more applications. Apart from these many tasks the other function which can be carried out in the future by working on the other different protocols apart from the protocols which are been used here as a concept of dropping and accepting the particular packets depending on the instructions or the rules given to it. A rule is also been configured such that the packets are dropped for a period of time and also at some regular intervals of time.

References

[1] Chirsoph L.Schuba, Ivan.krsul, Markus G.Kuhn, Eugene H.Spafford, Aurobindo Sundaram, diego zamboni, Analysis of a Denial of Service Attack on TCP, COAST

Laboratory Department of Computer Sciences Purdue University 1398 Department of computer west Lafayette, IN 470907 – 1398.

[2] Defense Against TCP SYN Flooding Attacks - Wesley M. Eddy, Verizon Federal Network Systems.

[3] Packet filtering HOWTO – (www.netfilter.org/documentation/HOWTO/packetfiltering-HOWTO > html)

[4] Netfilter framework - http://en.wikipedia.org/wiki/Netfilter

[5] Friendly ARM Board - www.friendlyarm.net/products/mini2440

[6] Linux Firewalls Using Iptables – HOWTO -http: // www.linuxhomenetworking.com /wiki/index.php/Quick_HOWTO:Ch14:Linux_Firewalls_Using_iptablesJ. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.