Implementation of Web Security using Packet-Scrutinizing Router

Muhammad Akram[1], Muhammad Imran Shafi[2], Muhammad Hamid Fayaz[3], and Sikandar Hayat[4]
[1]*Abdul Razak Institute of Modern Languages & Computer Sciences, Mirpur AK Pakistan*
2Nackademin YRKESHÖGSKOLA, Stockhlom, Sweden
[3,4]*Blekinge Institute of Technology SE-371 79 Karlskrona, Sweden*
akram.moghal@gmail.com, cancerbyname@hotmail.com, mhfa06@student.bth.se, sih@bth.se

Abstract— Network security has becomes more and more critical to securing the business application. Organizations need to incorporate security into the network design and infrastructure. World Wide Web is available with sensitive and business information. This information opens the lots of opportunities and possibilities of attack by the thieves, and can vandal and misuse by your own employees as well. To secure the systems which are connected to a network or the Internet, there is a need of certain protection from incoming and outgoing threats. In this paper we have described how packet filtration is done on the base of the IP address, to discard or accept any in-coming packet into the network. Also this paper will provide the guidance for network managers how to plan and implement security with the help of packet scrutinizing routers.

Index Terms—Firewall, Protocol, Packet filtration, Network, Web Security, Router.

I. INTRODUCTION

Today the actual risk for a business man is the loss of important data, when they connect with the world through Internet. Internet can enhance communication ways when your employees connect through remote access. Internet may open the door of world to communicating with customers and suppliers, and access to internet is a massive source of information.

Security on web is essential for the organization to secure their businesses, competitive information and financial records etc. The simple TCP/IP could not provide full security for organization. Organizations need to protect their Intranet and Internet network from the exterior attackers using firewalls.

Packet based data communication networks is the invention of modern age. Where increase in malicious activities like hacking, cracking, intrusion and disruption are predatory elements. So by targeting certain nodes using these activities it is possible to take down the entire network. Large scale ISP´s and NSP´s use packet scrutinizing router as firewalls in order to implement Web Security for the users. These packet scrutinizing routers read header information before forwarding each data packet to the destination.

In this paper we have discuss some different Web Security aspects, firewalls, protocols and packet scrutinizing routers. At the end, this paper illustrates a case study of CISCO routers, how we can plan and implement packet-scrutinizing router within the network. Also this paper tells some advantages and disadvantages of packet-scrutinizing router.

II. ASPECTS OF WEB SECURITY

Mostly every business requires security over the Internet. Apart from secure messaging, privacy and security of local resources have to be conserved. Secure transmission of information over the Internet has following main aspects as following [1, 2]:

- Authentication
- Authorization
- Confidentiality
- Privacy
- Availability
- Integrity
- Non-Repudiation.

Where as these security aspects can be further elaborated as follows [1, 2]:

Authentication is the process of proving the identity of the entities that are communicating over the network/Internet. It can be verified by username/Id and password. Authentication ensures that only authorized person can access data/information from the network/Internet.

Authorization is process of ensuring the level of access for any authenticated user to access the secure information over the network/Internet. It grants or denies the access to particular information for authenticated user on the base of its identity.

Confidentiality is process of ensuring that no one can read the message except the authorized receiver. For secure transmission encryption techniques are applied.

Privacy is technique for handling the data like personal details e.g. credit card numbers, pin-code etc but also files that stores on intranet. That kind of data could not be access by any unauthorized person.

Availability ensures that user can access the data/information when he/she need or want to use it. It does not mean that availability is only related to the information/data but also related to the availability of other system resources.

Integrity is assuring that the original contents of the received information have not been changed during the communication over the insecure channel.

Non-repudiation is a mechanism to prove that the sender really sent this message.

III. FIREWALLS AND PROTOCOLS

To secure the systems which are connected to a network or the Internet, our network need certain protection from incoming and outgoing threats. Firewalls can be used to protect the system from these threats. Firewalls scrutinize the data packets those come inside or outside in the network, on the bases of this scrutinizing check it makes the decision to pass or discard data packet. [3]

Firewall can be in the shape of a hardware device or a software program that secures the network. Hardware firewall is a device which is installed in Intranet as shown in figure1, and software firewall is available in shape of software program as shown in figure 2. [4]

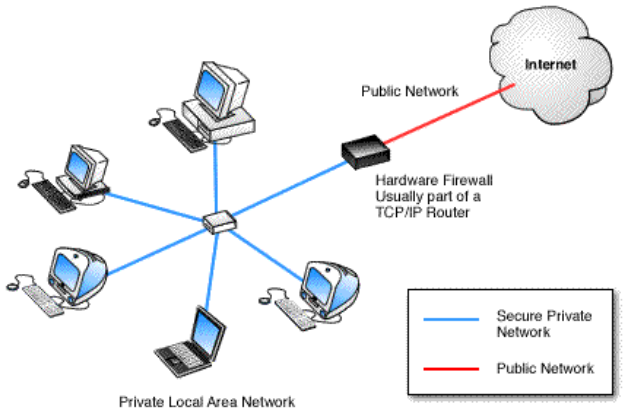

Fig 1 Hardware Firewall

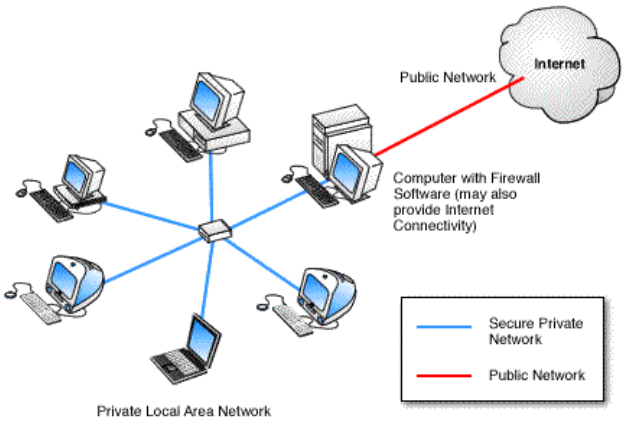

Fig 2. Software Firewall

A. Types of Firewall

There are three main types of firewalls

- Packet Filtering Routers
- Application Level Gateway
- Circuit Level Gateway

Packet Filtering Routers

Packet filtering is a technique can be used as an instrument to implement the wide range of policies in the network. The actual purpose for implementing these policies is to secure the network from unauthorized access.

Packet filtering techniques perform parsing on the header of any packet and then apply some rules, which make the decision to allow the packet or discard it as shown in figure 3.

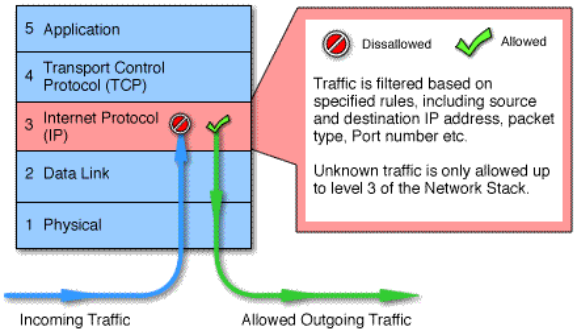

Fig. 3 Packet Filtering Firewall [4]

The header fields of any packet which are available for filtering are type of packet (TCP, UDP, etc), IP address of source machine, IP address of destination machine and destination port. [5]

Application Level Gateway

In application level gateway packets are sort out at the application layer of the OSI reference model and then decision is made to pass the packet or discarded as shown in figure 4.

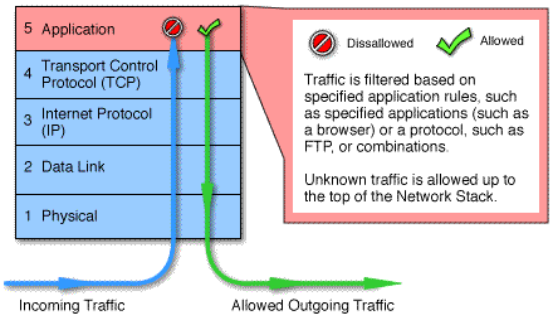

Fig 4. Application Level Gateway [4]

We can say that Application level gateway as proxy server, because proxy code is implement at the gateway for the any application. If any user wants to access the remote host, first he/she will contact with the gateway using any TCP/IP application. User will give the name of the remote host with his/her user ID and all authentication information to the gateway. Gateway will then make possible the communication between these two endpoints. [6]

Circuit Level Gateway

Circuit level gateway work at session layer of OSI model or TCP layer of TCP/IP model' as shown in figure 5. [4]

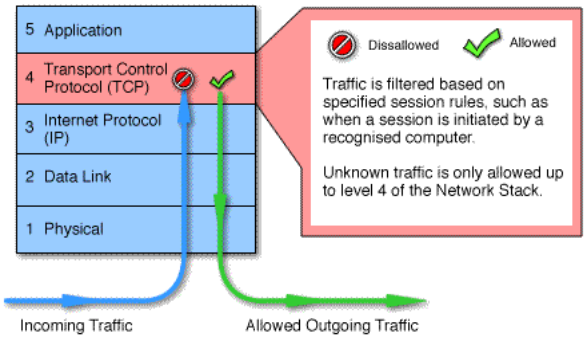

Fig. 5 Circuit Level Gateway [4]

In circuit level gateway, Gateway makes two TCP connections because one end-to-end TCP connection is not possible in this technique. First connection is between itself and the inner-host. Second connection is between itself and the outer-host. When these two connections are set up then gateway sends the TCP segments between these two nodes. Gateway did not check/filter contents of these segments during the communication. For maintaining the security there will be some functions, these functions make the decision that which connections are allowed and which are not allowed. [6]

B. Security Protocols

Many types of security protocols have been developed to prevent WWW against threats. Most of cryptographic techniques are used for end-to-end web security. TCP/IP protocol suits stipulate security protocols to run on different layers. Both good and bad feature of a protocol on a particular layer can watch during implementation. Network layer has an advantage to implement security which is apparent form end user. At the other way, it could need additional processing operating cost in network devices e.g routers. [7] To understand how firewalls work, network manager need to learn about how different layers work together on network. Every layer has own tasks in a seven layer network architecture model. A protocol may travel one or more physical layer (layer one) as layer one separate from the other protocol layers (three to seven). A physical cable may transmit one or more protocol [4].

At different layers, firewalls use different way to control insecure traffic. A firewall may work at lowest layer that is layer three, and called network layer in OSI model and Internet Protocol layer in TCP/IP. This layer is responsible for routing the packets to their end points. In a firewall, this layer is only verified which packet is coming from a secure or reliance source or not. Other type of firewalls that are operate with transport or application layers that know more about the packets and may be very careful to allow access [4].

Application Layer offer patterns in end-application for the end-user during such as file transfer (FTAM), virtual terminal service (VTS) and electronic mail to interrelate the transmission of a network [8]. In TCP/IP, This layer collaborates with transport layer to receive and send data. Application layer deals with Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) [7].

Transport layer is responsible for data transferring between applications and also for data reliability and integrity [7, 8]. HTTP, IMAP and Secure Socket Layer (SSL) high level protocol are available in this layer for high level security [4, 7].

Network Layer gives many advantage in implementing the security e.g confidentiality and integrity of the packets. IP Security protocol and different set of RFCs (Request For Comments) are included in this layer [7, 8].

Data link layer define the different strategies for accessing and sharing the physical channels on a network. Ethernet (IEEE 802.3), Token Ring (802.5), Point-to-Point Protocol and Point-to-Point Tunneling Protocol (PPTP) are the example that used in this layer [7, 8].

IV. TRAFFIC CLASSIFICATION

"*Classification determines the per-hop behaviors and traffic conditioning functions, such as shaping and dropping, which are to be applied to the packet. Classification of packets can be based on the DS field or IP Precedence in the packet header. Classification can be based on other IP header fields, such as IP Source Address (SA), Destination Address (DA), and protocol, or on fields in the packet payload, such as port number. Classification can also be based on ingress interface. It is possible to base classification on Multi-Field (MF) criteria such as IP source and destination addresses, protocol, and port number*" [9].

A. Packet Filtration

Access Control List (ACL) is a technique use to filter non-demanding or irrelevant traffic from the network [10].

ACL techniques are used to reduce the traffic. To reduce unwanted traffic there are two following types of ACL that can be applied in different scenarios:

- Standard IP Access List
- Extended IP Access List

Standard IP Access List

Standard IP access-list consists of commands to filter packets on the basis of their source address. Every crossing packet is filters on the bases of these commands and hence permitted or denied by a standard IP access list.

To provide a clear picture of policy making, some labs are included in this report which provides a clear understanding of traffic filtration.

Lab#1: (Implementation of access-list on Source IP Address)

Lab1 demonstrates the configuration overview of given scenario in figure 6, which shows restricting incoming traffic based on source IP address using IP standard Access-list. RouterA is connected serial via crossover cable with RouterB. RouterA has an interfaces defined on Ethernet 0. Both Routers are configured for RIP.

In this lab the access-list 1 will be applied to the serial0 interface of RouterA to restrict the incoming traffic from RouterB.

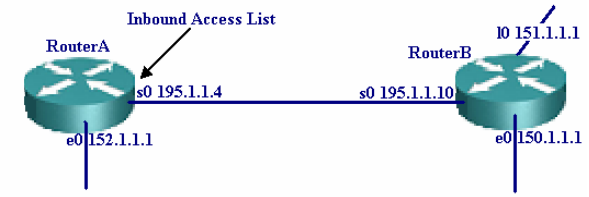

Fig 6. Inbound standard access list on the serial0 interface of RouterA

The configurations for the two routers used in the scenario are as following (key access list configurations for RouterA are highlighted in bold) as shown in figure 6.

Configuration of Router(A)
hostname RouterA
interface ethernet0
ip address 152.1.1.1 255.255.255.0
interface Serial0
ip address 195.1.1.4 255.255.255.0
ip access-group 1 in ← Applies access- list 1 to all inbound traffic on serial 0.
ip route 150.1.1.0 255.255.255.0 Serial0 ← Static route is used because no dynamic routing protocol is configured.
Access-list 1 permit 150.1.1.0 0.0.0.255 ← Defines access-list (1) permitting traffic from wildcard mask network 150.1.1.0.
(Note: all other access implicity denied) ← **All access-lists end with an implied deny all**.
end.

Monitoring and Testing
To test the configuration, ping RouterA (195.1.1.4) using the extended ping command on RouterB, and source the packet from the loopback interface (151.1.1.1). To use this command, simply type ping at the privileged level.

RouterB # ping
Protocol [ip]:
Target IP address: 195.1.1.4
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 151.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose [none]:
Sweep range of sizes [n]:
Monitor incoming packets on RouterA using the debug ip packet command. The output from this command is shown as following. Notice that the packet is being denied and an ICMP host unreachable message is sent back to RouterB.
IP: s=151.1.1.1 (Serial10), d=195.1.1.4, len 100, access denied
IP: s=195.1.1.4 (local), d=151.1.1.1 (Serial10), len 56, sending ← Host unreachable message.
The output from the command show access-list 1 on RouterA is shown as follows. Note that the wildcard mask permits all host on network 150.1.1.10.
RouterA# show ip access-lists 1
Standard IP access list 1

Permit 150.1.1.0, wildcard bits 0.0.0.255

Extended IP Access List
Extended access-list is a procedure through which packets can be denied or permitted based on source and destination IP address, port numbers and upper-layer protocols. Due to these enhance functionalities it is known as extended access list.

LAB#2: (Extended IP Access-List on inbound serial interface)

Lab2 demonstrates the configuration overview of given scenario in figure 7, which shows restricting incoming traffic based on source and destination IP addresses using IP extended Access-list. RouterA is connected serial via crossover cable with RouterB.
In this lab the access-list 100 will be applied to the serial0 interface of RouterA to restrict the incoming traffic from RouterB. All other traffic will be routed using the normal routing process.

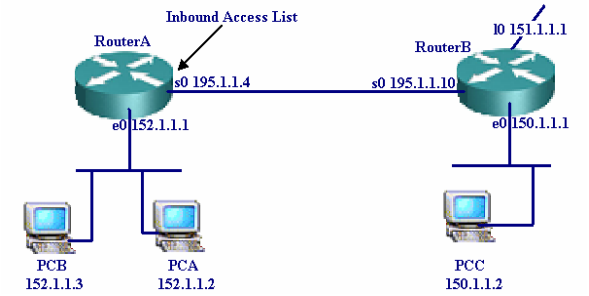

Fig 7. Inbound extended access list on the serial0 interface of RouterA.

The configurations for the two routers in this lab2 are as follows (key access list configurations for RouterA are highlighted in bold):

Configuration Router (A)
hostname RouterA
interface Ethernet0
ip address 152.1.1.3 255.255.255.0 secondary
interface Serial0
ip address 195.1.1.4 255.255.255.0
ip access-group 100 in ← Applies access-list 100 to all inbound traffic on serial 0.
specific is the same as wildcard mask 0.0.0.0
Access-list 100 permit ip host 150.1.1.2 host 152.1.1.2 log ← Generates an informational
Permit any IP packet from 150.1.1.2 to logging message about any packet that matches the entry.
Access-list 100 deny ip host 150.1.1.2 host 152.1.1.3 log ← Generates an informational Deny any IP packet from 150.1.1.2
(Note: all other access implicitly denied) ← **All access-list end with an implied deny all.**
end

Monitoring and Testing
All of the following examples use the extended ping command on RouterB to source the packets from the secondary IP addresses defined in the configuration. This command is used instead of multiple PCs on RouterB's LAN.
From RouterB, ping 152.1.1.3 using source address 150.1.1.2.
From the output of the debug ip packet command on RouterA, we see that the packet is being denied and that an ICMP host unreachable message is being sent.
IP: s=150.1.1.2 (Serial0), d=152.1.1.3, len 100, access denied
IP: s=195.1.1.4 (local), d=150.1.1.2 (Serial0), len 56, sending ← ICMP host unreachable

The output of following commands after execution shows which access lists are defined and the number of matches against each one.

RouterA# **show ip access-lists**
Extended IP access list 100
Permit ip host 150.1.1.2 host 152.1.1.2 log (5 matches)
Deny ip host 150.1.1.2 host 152.1.1.3 log (**105 matches**)

From RouterB, ping 152.1.1.3 using source address 150.1.1.3 using source address 150.1.1.2
From the output of the **debug ip packet** command on RouterA, we see that the packet is being permitted.
The output of following command after execution shows which access lists are defined and the number of matches against each.

RouterA# **show ip access-lists**
Extended IP access list 100
Permit ip host 150.1.1.2 host 152.1.1.2 log (308 matches)
Deny ip host 150.1.1.2 host 152.1.1.3 log

V. Advantages and Disadvantages of Packet Scrutinizing Router

Packet scrutinizing routers have some advantages and disadvantages.

A. Advantages

Implementation of packet scrutinizing router is not to much complicate if we compare it with other network security mechanisms.

Due to direct connection between internal and external hosts, data can be transfer at high speed.
In packet scrutinizing routers, use of client application is easy because packet checking is done at the router level.

B. Disadvantages

In packet scrutinizing routers setting up the complex rules for security is difficult.
Because user connects directly from network to network, so in this way it leaves some useful information (such as user address, access information) at risk.
Packet scrutinizing routers did not provide facility for authentication in case of specific user. It only discard or give access right to packet on the base of source or destination addresses or port address.

VI. Cisco AAA Security Solutions

Cisco AAA security solutions gives us important steps for the preparation and implementation of authentication, authorization, and accounting (AAA). [11]
Network manager can select a security solution, Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-in User Service (RADIUS), depending upon the requirement of a network design [11].

A. TACACS+ Vs RADIUS

TACACS+ is more secure than RADIUS because it encrypts the whole body of packet using TCP, but RADIUS encrypts only password using UDP.
RADIUS does not segregate authentication and authorization, but TACACS+ check authentication, authorization and accounting separately.
RADIUS does not provide support for multi protocols, but TACACS+ does.

RADIUS does not provide facility for user to control the commands which are executed on router, but in TACACS+ user can control router command on the base of per user or per group.
TACACS+ is useful for the management of the router and terminal services but RADIUS is not [11].

B. Network Planning for Cisco AAA Packet Scrutinizing Routers

For planning AAA security, network manager should consider following checklist as shown in table 1 [11].

TABLE 1
AAA SERVICE DEFINITION CHECKLIST ACCESS [11]

Network AAA Checklist Questions	Access Network Policy
What AAA protocols do you plan to deploy?	RADIUS and TACACS+
Where do you want the users' passwords to be stored?	External Oracle database
Do you plan to support one-time passwords? If so, what tool do you plan to use to support this requirement?	No
Do you intend to implement database replication?	No
Do you require support for token caching?	No
What type of accounts currently exists?	UNIX, NT
Do you plan to implement an AAA server? If so, on which product?	Yes, Cisco Secure for UNIX
What database do you plan to use?	External, Oracle

C. Security Implementation Cisco AAA Packet Scrutinizing Routers

For implementing security on AAA routers network manager keep in mind the following checklist which is shown in table 2 [11].

TABLE 2
AAA SECURITY CHECKLIST ACCESS [11]

Network AAA Checklist Questions	Access Network Policy
What is the current security policy for passwords?	PAP for dial-in PPP users CHAP passwords for dialup routers DES passwords for router administrators
What services will be denied?	Concurrent sessions for dial-in users EXEC shell access for dial-in PPP users Access to specific hosts within the corporate intranet work Access to specific network services, such as Telnet, FTP, and rlogin
What type of mechanism will exist if AAA server is down?	Local privilege level 15 account Authentication and authorization disabled on console port
Are local accounts allowed in routers and NASs?	Yes
What accounting information is required?	Username Privilege level of clients Session start and stop times Elapsed time Privilege level 15 command usage Configuration changes Failed log in attempts Failed command authorizations
What type of accounting mechanism will be used?	Customer written SQL query to Oracle database
Who is responsible for reviewing daily logs?	Network managers
Will users be allowed concurrent sessions?	Dialup PPP = No Dialup router = Yes Router administrator = Yes

What type of administrative access will be assigned to router administrators?	Full control assigned to senior router administrators Basic control assigned to junior router administrators Customized command control for mid-level router administrators
Support for Multilink?	Yes

VII. CONCLUSION

This paper focuses on which points, network manager should keep in mind when planning or implementing the AAA Security on routers. Network manager can select a security solution, Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-in User Service (RADIUS), depending upon the requirement of a network design. TACACS+ is more reliable then RADIUS.

Access Control List (ACL) is a technique use to filter non-demanding or irrelevant traffic from the network.

Packet scrutinizing routers is good choice to implement the security, it scrutinize all incoming and outgoing packet and discard those packets that violate the predefined rules. Also it is not very complicated to implement

VIII. REFERENCES

[1] Martin Wimmer, Alfons Kemper & Stefan Seltzsam, Web Engineering: The Discipline of Systematic Development of Web Applications", John Wiley & Sons, Ltd., West Sussex, England.

[2] Shweta Bhasin, 2002, Web Security Basics, Course Technology.

[3] Sunil Hazari. Nov 6, 2000, 'Firewalls For Biginners', 21 April 2007, www.securityfocus.com/infocus/1182

[4] PCNET, Firewalls, 21 April 2007. http://support.pcnet.ca/

[5] Brent Chapman, D, September 1992, 'Network (In) Security Through IP Packet Filtering', Proceedings of the Third USENIX UNIX Security Symposium, Baltimore, MD.

[6] William Stallings, Network Security Essentials Applications and Standards, Addison Wesley, Longman Singapore.

[7] Ari Niemi, 'End-to-End web security-protocols overview', 24 April 2007.

[8] Renqi Li & E.A. Unger. Summer 1995, 'Security Issues with TCP/IP', Special issue on security, Volume 3 , Issue 1, Pages: 6 – 13, 26 April 2007, ACM SIGAPP Applied Computing Review.

[9] S. Poretsky, J. Perser, S. Erramilli, S. Khurana, October 2006, Terminology for Benchmarking Network-layer Traffic Control Mechanisms, 27 April 2007. http://www.rfcarchive.org/getrfc.php?rfc=4689#top

[10] Access Control List, 27 April 2007, http://en.wikipedia.org/wiki/Access_control_list

[11] Cisco AAA Case Study, 28 September 2002, Cisco, http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/secsols/aaas ols/c262c1.htm