© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

A Review: Enhancing Security Of Network System Using Ip Filter And Cryptography

[1]Sheenu Sachdeva ,Research Scholar, Department of CSA, CDLU Sirsa, ssheenu75@gmail.com
[2]Er. Shilpa Jain, Asstt. Prof. Department of CSA, CDLU Sirsa, engishilpa19@gmail.com

Abstract- In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules [1]. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Routers that pass data between networks contain firewall components and can often perform basic routing functions as well. Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network [2]. In this research we have enhanced security of network at host-based firewall using One time password generation, We use the concept of socket programming (ip address+ port no.) with client server model. Also we enhance the cryptographic mechanism using the RSA algorithm. so here is three layer security we provide to our network during message transmission. This work done at host-based firewall.

Keyword: DHCP, VPN, RSA, OTP, IP, SOCKET PROGRAMMING.

1. Introduction

The term firewall originally referred to a wall intended to confine a fire or potential fire within a building. The predecessors to firewalls for Packet filters [5] act by inspecting the "packets" which are transferred between computers on the Internet. If a packet does not match the packet filter's set of filtering [11] rules, the packet filter will drop (silently discard) the packet or reject it (discard it, and send "error responses" to the source). Conversely, if the packet matches one or more of the programmed filters, the packet is allowed to pass. This type of packet filtering is done by socket programming (ip address+ port no.). The endpoint in an inter process communication is called a socket. Sockets are UNIQUELY identified by Internet address, end-to-end protocol, and port number. That is why when a socket is first created it is vital to match it with a valid IP address and a port number. The data transmission between two sockets is organized by communications protocols, usually implemented in the operating system of the participating computers Packet filtering firewalls[7] work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers. When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the packet filtering rules that are configured in the firewall and drops or rejects the packet accordingly. When the packet passes through the firewall, it filters the packet on a protocol/port number basis (GSS). For example, if a rule in the firewall exists to block telnet access, then the firewall will block the TCP protocol[12] for port number 23.We done the packet filtering using socket programming with client server model. The server executes first and waits to receive; the client executes second and sends the first network packet to the server. After initial contact, either the client or the server is capable of sending and receiving data. For many common services, standard port numbers are defined. Ports 0 – 1023, are reserved and servers or clients that you create will not be able to bind to these ports unless you have root privilege [2]. Ports 1024 – 65535 are available for use by your programs, but beware other network applications maybe running and using these port numbers as well so do not make assumptions about the availability of specific port number.

2.Review of Literature

1. **Neetu Settia et. Al (2012) discussed the security and attack aspects of cryptographic techniques[1]**
Security and attack aspects of cryptographic techniques and also discussed the dominant issues of security and various attacks. Finally, bench marked some well-known modern cryptographic algorithms in search for the best compromise in security. In this paper, CrypTool was used as a simulator to conduct the experiments and to get the result.

2. **Sanchez-Avila et.al (2013) analyzed the structure and design of Rijndael cipher[2]**
Analyzed the structure and design of Rijndael cipher (new AES), remarking its main advantages and limitations, as well as its similarities and dissimilarities with DES and T-DES. Finally, a performance comparison among new AES, DES and T-DES for different microcontrollers has been carried out, showing that new AES have a computer cost of the same order than the one needed by T-DES. A. Murat Fiskiranet.al showed some cryptographic algorithms that have properties that make them suitable for use in constrained environments like mobile information appliances, where computing resources and power availability are limited characterization of the instructions executed by these algorithms, and demonstration that a simple processor is sufficient.

3.**Punita Meelu et.al (2014) presented the[3]** Fundamental mathematics behind the AES algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security since AES provides better security and has less implementation complexity and has emerged as one of the strongest and most efficient algorithms in existence today.

4. **Susan et.al (2015) concluded that the Security field is a new, fast moving career [4]**
A focus on security stabilizes course material, reduces worry about student hacking, and helps to provide students the skills necessary to become security analysts. It also defines the set of skills required by Network Security analysts as network Security skills emphasize business practices, legal foundations, attack recognition, network optimization and describes active learning exercises that assist the students in learning these important skills. This actually summarized all the skills relating to network security, and discussed active learning exercises that assist students in learning these important skills. Main focus was on security information skills that are to be used in securing the network

5.**Murray (2015) presented a survey of SSL servers[5]**
Murray's survey generally covered similar issues as in this paper, though in less detail. In addition, it also considered whether or not a server's certificate was expired or self-signed. Murray defined weak servers to be those that supported at least one of the following flaws: 1) only supports SSL2.0; 2) only supports symmetric encryption using keys with at most 56 bits; 3) only supports certificate key sizes of at most 512 bits; 4) uses an expired or self-signed certificate. Murray defined strong servers to be those that supported all of the following properties: 1) supports SSL 3.0 or TLS (can support

SSL 2.0); 2) supports symmetric encryption using keys with at least 64 bits (can support 40-bit keys); 3) supports certificate key sizes of at least 1024 bits (can support smaller certificate keys).

3 .Research Methodology

The present research work is experimental in nature where the work has been done to provide security to the data delivered from client to server using socket programming.

Objectives of the research are :
1. To implement packet filtering concept and socket programming
2. To enhance security mechanism using OTP.
3. To use firewall to filter the unauthentic data transmission over network [11].
4. To enhance the network security of Digital Data by adding Security Mechanisms [12].

We use the concept of socket programming at the host-based firewall in which clients are connected with server using ip address (client) and port number (server), clients which are connected to the server only able to receive the data from the server. Sockets provide the communication mechanism between two computers using TCP. A client program creates a socket on its end of the communication and attempts to connect that socket to a server. When the connection is made, the server creates a socket object on its end of the communication. The client and server can now communicate by writing to and reading from the socket. [12] We maintained a database at server site in which clients status are mentioned , the clients with status '1' are only able to receive the data and decrypt the message .this means packet filtering is also done with socket programming. We are using ip filter to reject unauthenticated transmission of packets from server to client. We have to enhance network security by customizing existing encryption techniques [6].One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or cryptosystem. Cryptosystems are designed to provide particular functionality (e.g. public key encryption) while guaranteeing certain security properties. Cryptosystems use properties of underlying cryptographic primitives to support system's security properties. Of course, as distinction between primitives & cryptosystems is somewhat arbitrary, a sophisticated cryptosystem could be derived from a combination of several more primitive cryptosystems. RSA algorithm is sometimes considered a cryptosystem, & sometimes a primitive.

4. Conclusion

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. For this packet filtering is done with the help of socket programming. Such system would be more secure & would help in reducing loop hole of existing security mechanisms.

5. References

[1] Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". Communications of the ACM **40** (5): 94. doi:10.1145/253769.253802.
[2] "What is Firewall?". Retrieved 2015-02-12.
[3] Definition of Firewall, Check Point Resources
[4] Andrés, Steven; Kenyon, Brian; Cohen, Jody Marc; Johnson, Nate; Dolly, Justin (2004). Birkholz, Erik Pack, ed. Security Sage's Guide to Hardening the Network Infrastructure. Rockland, MA: Syngress. pp. 94–95. ISBN 9780080480831.
[5]The OpenSSL project.http://www.openssl, org
[6] Canavan, John E. (2001). Fundamentals of Network Security (1st ed.). Boston, MA: Artech House. p. 212. ISBN 9781580531764.
[7] Liska, Allan (Dec 10, 2014). Building an Intelligence-Led Security Program. Syngress. p. 3. ISBN 0128023708.
[8] Ingham, Kenneth; Forrest, Stephanie (2002). "A History and Survey of Network Firewalls" (PDF). Retrieved 2011-11-25.
[9] Firewalls by Dr.Talal Alkharobi
[10] Peltier, Justin; Peltier, Thomas R. (2007). Complete Guide to CISM Certification. Hoboken: CRC Press. p. 210. ISBN 9781420013252.

[11] Ingham, Kenneth; Forrest, Stephanie (2002). "A History and Survey of Network Firewalls" (PDF). p. 4. Retrieved 2011-11-25.

[12]Michael J.Wiener. performance comparison of public ky cryptosystem.
http://www.reasecurity.com