International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206610

Enhancing the Network Security Using Multilayer Security Features

Deepinder Singh Sran[1], Er. Sheenu Sachdeva[2]
[1]Student, The Sirsa School Sirsa Haryana, India
[2]Assistant Professor, Department of Computer Science, JCD Memorial College, Sirsa, Haryana, India

Article Info
Volume 6, Issue 6
Page Number: 83-86
Publication Issue :
November-December-2020

Article History
Accepted : 10 Nov 2020
Published : 18 Nov 2020

ABSTRACT

With the occurrence of the World Wide Web and the emergence of ecommerce applications and social networks, organizations across the world generate a large amount of data daily. Information security is the most extreme basic issue in guaranteeing safe transmission of data through the web. Also network security issues are now becoming important as society is moving towards digital information age. As more and more users connect to the internet it attracts a lot of cyber-attacks. It required to protect computer and network security i.e. the critical issues. The pernicious hubs make an issue in the system. It can utilize the assets of different hubs and safe guard the assets of its own. In this paper we provide an overview on Network Security and various techniques through which Network Security can be enhanced i.e. Cryptography. Cryptography and Network Security is used to protect network and data transmission takes place over wireless network.

Keywords : Security, Threats, Cryptography.

I. INTRODUCTION

The predecessors to firewalls for Packet filters act by inspecting the "packets" which are transferred between computers on the Internet[5]. This type of inspecting of packets 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, endto-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. If a packet does not match the packet filter's set of filtering rules[7], the packet filter will drop (silently discard) the pac ket 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. Packet filtering firewalls 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 [11]. 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 for port number 23[12].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. The data transmission between two sockets is organized by communications protocols, usually implemented in the operating system of the participating computers

II. REVIEW OF LITERATURE

1. Murray (2015) presented a survey of SSL servers [1] 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). 2.Sanchez-Avila et.al(2014) 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 Fiskiran et.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. Susan(2013) et.al concluded that the Security field is a new, fast moving career[3] 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 4. Neetu Settia(2012) et. al discussed the security and attack aspects of cryptographic techniques[4] 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. 5. Zhang et.al (2011) focused on[5] Application level attacks and explores how the packet payload can be used for identifying application level attacks. It also discusses the current status of network anomaly detection, and emphasized the importance of payload based detection research using existing problems, and proposed an efficient method to detect payload related attacks. The method is divided into a training phase and a detection phase

III. 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 this research are: To implement the packet filtering concept• and socket programming. To enhance security mechanism using OTP.• To use firewall to filter the unauthentic data•

transmission over network. To enhance the network security of Digital• Data by adding Security Mechanisms. We implement the concept of packet filtering act by inspecting the "packets" which are transferred between computers on the Internet. And we perform the packet filtering by 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. 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 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. RSA algorithm is sometimes considered a cryptosystem, & sometimes a primitive

IV. CONCLUSION AND FUTURE WORK

Security is a very complex topic in our computing system. It is very important to build systems and network in such a way that the user is not constsntly remainded of the security system around him because it is responsible for securing all information passed through networked computers. For this we introduce the system concept in which packet filtering is done with the help of socket programming by creating a socket component at both server end and client end then communication take place. Such system would be more secure & would help in reducing loop hole of existing security mechanisms. Unauthentic person would be unable to decrypt data as IP Address of person would be confirmed before decryption. Server & client both sides would be programmed using socket programming. So due to presence of our own secure protocol cryptanalyst would be unable to decrypt data even if he has stolen decryption Key. The research work has been implemented successfully where socket programming played a vital role in providing secure transmission of file in encrypted form from server to client. In present work we made a single machine as client as well as server therefore one sided transmission of files are possible at one time either from client to server or from server to client. In future we will try to implement this concept on more than one machine and two sided transmission will be implemented and the socket programming concept will be implemented with more powerful features for transferring data on different machines.

V. 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 Open SSL project. http://www.openssl,org
[6]. Firewalls by Dr.Talal Alkharobi

[7]. Peltier, Justin; Peltier, Thomas R. (2007). Complete Guide to CISM Certification. Hoboken: CRC Press. p. 210. ISBN 9781420013252.
[8]. Ingham, Kenneth; Forrest, Stephanie (2002). "A History and Survey of Network Firewalls" (PDF). p. 4. Retrieved 2011-11-25.
[9]. Michael J.Wiener. performance comparison of public ky cryptosystem. http://www.reasecurity.com

Cite this article as :

Deepinder Singh Sran, Er. Sheenu Sachdeva, "Enhancing the Network Security Using Multilayer Security Features", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 6, pp. 83-86, November-December 2020. Available at doi : https://doi.org/10.32628/CSEIT206610
Journal URL : http://ijsrcseit.com/CSEIT206610