A Secured Communication between Web Servers in a Network

P.T.Kasthiribai¹, M.Sundararajan²

¹Research scholar, Bharathiar University, Head of the C/S Dept., ThiruthangalNadar College, Chennai
²Research Supervisor, Bharathiar University, Assistant Professor, Nandam Arts College for men, (Autonomous), Chennai

Email: kasthiript@rediffmail.com, drmsrajan23@gmail.com

Abstract-To secure the communication between web servers there are different methods used to protect the communication and data. Confidentiality in Web communications can be achieved by using an encrypted, secure channel. End to end authentication can be done using routing protocols. To establish a secured channel between two end points, Source authentication, Data integrity and data confidentiality and Protection against replay attack are the security features used. A secured communication is achieved from client to IIS, between the web servers and within web servers. In this paper three methods namely core defense, boundary defense and distributed defense are dealt with in order to secure the communication so that illegal access to data, unauthorized access to data and DDoS attack in a network can be avoided. In order to achieve data integrity, confidentiality and security the communication between web servers is secured.

Keywords- DDoS (Distributed Denial of Service), SYNa(Synchronization),ACK (Acknowledgement), WS1 (Web Server1), WS2 (Web Server2), IIS (Internet Information Server), SSL (secure socket layer), IDS (Intrusion Detection System).

I. INTRODUCTION

Security is a major concern in data communication. Between web servers there should be a secured communication otherwise data will be misused, manipulated and stolen. Careful data communication makes the web server to do its task perfectly. For sending sensitive information, the communication must be secured. To secure the information HTTPS (hypertext transfer protocol secure), SSL (secure socket layer) protocol can be added. HTTPS uses long-term public and secret keys to exchange and a short term session key to encrypt the data flow between the client and the server. This paper analyses where to use SSL, HTTPS, IPSec protocols, SYN-cookies so that the information can be secured.

The paper is organized as follows. Section II summarizes the related previous works. Section III describes proposed system and the architecture. Section IV describes protection from DDoS attack. Section V concludes the paper.

II. RELATED WORK

Security on the endpoints (client-server, or client-client for peer-to-peer) is an absolute requirement for securing the communication [3]. Such a solution contains the following components: Identity: This component encompasses known and verifiable entity identities on both ends; note that an identity can be temporary for a connection. Protocols (for example, TLS [1] and IPSec [2]): Protocols are used to dynamically negotiate session keys, and to provide the required security functions. Algorithms: Advanced Encryption Standard [AES][5], [9] Triple Digital Encryption Standard (3DES) protect data in transit, for example through encryption or integrity checks. Secure implementation: The endpoint (client or server) that runs one of these protocols mentioned previously must be free of bugs that could compromise security. Secure operation: Users and operators have to understand the security mechanisms, and how to deal with exceptions. Enabling end-to-end secure communication between wireless sensor networks and the Internet [2].

III. PROPOSED SYSTEM

There are three stages of protection. They are:

1. Distributed defense
2. Boundary defense
3. Core defense

Distributed defense involves authentication, authorization and use of SSL [6]. Boundary defense include digital signature method. Core defense include IPSec protocol. By giving the protection in the above mentioned three ways, a secured communication is achieved from client to IIS, between the web servers and within web servers respectively. Further use of SYN cookies protects the data from DDoS attack.

A. Phase 1 – Boundary Defense

Figure 1 shows the communication between the client and the server. In this phase, the network boundary is protected by an IDS1 that uses a digital signature method.

B. Phase 2 – Distributed Defense

In this phase, to enter into another web server (WS2), the existing server (WS1) that wants to communicate, sends user name and password and knocks the firewall of the WS2. The WS2 checks who the user is and what rights the user has with the database. There exists a VPN between the two web servers which uses L2TP to manage the IP address assigned to the users. Further this firewall uses an Intrusion Detection System (IDS2) a Secure Socket Layer protocol between applications and the TCP/IP protocols. It provides server authentication and optional client authentication and encrypted communication channel between WS1 and WS2. SSL provides Server authentication that is based on the server’s authentication certificate. Clients can identify the server by its certificate and can choose to communicate with authenticated servers. Clients can detect whether an unauthorized entity is trying to impersonate a legitimate Web server. Both servers and clients can choose to trust only those certificates that are issued by a specific CA. The server and the client negotiate the cryptographic algorithms that are to be used. Here AES [8]
algorithm is used. They also negotiate the secret, shared session key that is used to secure communication.

C. Phase 3 – Core defense
Figure 2 shows the communication between an Application server and database server. In this use of IPSec protocol secures the communication. IPSec uses Internet Key Exchange (IKE) protocol to negotiate and establish a secured communication between two web servers. For eg. When the user purchases items on line, that application server can communicate with the database server of the bank for payment through online. In this IDS-3 Internet Protocol Security (IPSec) can be used to secure the data sent between two computers, such as an application server and a database server of that bank.

IPSec [4] is completely transparent to applications because encryption, integrity and authentication services are implemented at the transport level. IPSec provides message confidentiality by encrypting all of the data sent between two computers. It also provides mutual authentication between two computers. The communication to specific IP protocols and TCP/UDP ports can also be restricted.

An IPSec policy [1] consists of a set of filters, filter actions, and rules. A filter consists of:
i) A source IP address or range of addresses.
ii) A destination IP address or range of addresses.
iii) An IP protocol, such as TCP, UDP, or “any.”
iv) Source and destination ports (for TCP or UDP only).

Filters can also be mirrored on two computers. A mirrored filter applies the same rule on client and server computer (with the source and destination addresses reversed). A filter action specifies whether to permit or block the traffic. A rule associates a filter with a filter action. A mirrored policy is one that applies rules to all packets with the exact reverse of the specified source and destination IP addresses. This IPSec protocol handles spoofing [10], eaves dropping, session hijacking. Thus a protection within server and between server and from client to internet server is achieved.

A. Protecting the data from DDoS and worms
Making Use of SYN cookies in the firewall protects the data of web server from DDoS. SYN flooding is the most commonly used DDoS. From the spoofed address the attacker sends a series of TCP SYN packets in this attack. This flood can prevent servers from handling legitimate connection requests.

There exists a Firewall service module which generates SYN – ACK signal as a reply to the other web server’s SYN request. This reply has a Cookie in the sequence (SEQ) field of TCP header. This cookie is a MD5 algorithm for authentication of source and destination IP addresses and port numbers. The FWSM receives an ACK from client/web server1 and it authenticates and allows the connection to the server. The FWSM sends its own SYN packet to server. The server replies with an SYN-ACK. The FWSM sends ACK to the server and the connection is built.

V. CONCLUSION
The above graph shows the percentage of protection when only boundary defense is used 50% protection is achieved. When boundary and distributed defense are used 75% of protection is achieved. When all the three defenses are used 100% security is achieved. Thus a secured communication
between web servers ensures data integrity, confidentiality and security. The use of IPSec protocol prevents DDoS attack and protects the data. Further a study can be extended how IPSec uses cryptographic algorithm like RSA and AES, triple AES to ensure data integrity and security. My Sincere thank to the God, my husband and my research guide.

REFERENCES

[2] Enabling end-to-end secure communication between wireless sensor networks and the Internet by Hong Yu, Jingsha He, Ting Zhang, Peng Xiao, Yuqiang Zhang
[4] IPSec - an overview by Somesh Jha University Wisconsin