Secure Socket Layer (SSL)

- Vivek Bhave (111508015)

Introduction

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain confidential at any cost. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

Sequence of Actions

To be able to create an SSL connection a web server requires an SSL Certificate. Your web server creates two cryptographic keys - a Private Key and a Public Key. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) - a data file also containing your details. During the SSL Certificate application process, the Certification Authority will validate details and issue an SSL Certificate containing your details and allowing you to use SSL. Your web server will match your issued SSL Certificate to your Private Key. Your web server will then be able to establish an encrypted link between the website and your customer's web browser.

Information Present in SSL Certificates

An SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

Protocols

Following are the four protocols used during implementation of the SSL. They are used in the process in the order followed in this document.

1. Handshake Protocol

Phases:

1. Initialise cipher suite, compression method, protocol version
2. Server xchange certificate and request for client certificate
3. Client sends the certificate and verifies the certificate
4. Hash value - authenticate done

Different messages passed:

a. Client hello
b. Server hello
c. Certificate x.509
d. Certificate xchange
e. Certificate request
f. Server done
g. Client key xchange

h. Certificate verify
i. Finished

2. SSL Record Protocol

Application data is gone through following :

a. Fragments
b. Compression
c. MAC is generated (DSS/SHA)
d. Encryption
e. Append SSL record

For MAC:

Hash (Mac-write-secret || pad-2 || Hash (Mac-write-secret || pad-1 || seq-num || SSL compressed length || ssl compressed type || ssl compressed fragment))

Pad - 2 : 0101 0110 - 48 times for MD5 / 40 times for SHA-1
Pad - 1: 0011 0110 - 48 times for MD5 / 40 times for SHA-1

3. Change Cipher Specification Protocol

Pending state (0) to current state (1)

4. Alert Protocol

Some alert messages are generated while processing SSL

Fatal errors:

1. Unexpected _msg
2. bad_record _MAC
3. decomposition _failure
4. Handshake_failure

Warning:

1. Close_notify
2. No_certificate
3. Bad_certificate
4. Unsupported_certificate
5. Certificate_removed
6. Certificate_expired
7. certificate_unknown