ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
*Published By:* **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
March 2017,
Vol. 10, No. (1):
Pgs. 249-254

# Privacy Preservation and Data Security on Internet Using Mutual SSL

**R. S. CHOUHAN and S. SEBASTIAN**

Department of Computer Science, Master of Computer Application, Christ University, India.
*Correspionding author E-mail: heybaby2019@gmail.com

http://dx.doi.org/10.13005/ojcst/10.01.34

(Received: March 14, 2017; Accepted: March 18, 2017)

**ABSTRACT**

It is essential to maintain a ratio between privacy protection and knowledge discovery. Internet users depend daily on SSL/HTPS for secure communication on internet. Over the years, many attacks on the certificate trust model it uses have been evolved. Mutual SSL authentication shared verification alludes to two parties validating each other through checking the digital certificate so that both sides are guaranteed of the other's identity. In technical terms, it alludes to a client (web program or client application) authenticate themselves to the server (server application) and that server likewise confirming itself to the client through checking the general public key certificate issued by trusted Certificate Authorities (CA). Since confirmation depends on computerized Certificate, certification authorities, for example, Verisign or Microsoft Declaration Server are a critical part of mutual authentication process. From an abnormal state perspective, the way toward authenticating and setting up an encrypted channel using certificate-based mutual SSL authentication.

**Keywords:** SSL (Secure Socket Layer), HTTPS (Hypertext Transfer Protocol), Certificates Authority, Mutual SSL, Mutual Authentication, Client, Certificate.

## INTRODUCTION

In the current , the technologies have advanced so much that most of the people prefer using the internet as a medium to transfer data from one person to another person across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc.

The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat ? it poses i.e. The personal or confidential data can also be stolen or hacked in many ways.

Therefore, it becomes necessary to take data security into consideration, as it is one of essential factors that need attention during the process of data transferring. Information security fundamentally implies insurance of information from unapproved clients or programmer sand giving high security to avert information change. This region of information security has increased more

consideration over the current time frame because of the huge expanding information exchange rate over the web.

In order to improve the security features in data exchanges over the internet, many techniques have been created like: cryptography, steganography and digital watermarking. While cryptography is a strategy to cover data by encoding it to figure messages and transmitting it to the proposed recipient utilizing an obscure key, steganography gives encourage security by concealing the figure content into an apparently undetectable picture or different configurations.

We will have a snappy outline and after that talk about 1-way and 2-way SSL. SSL ought to be the initial phase in securing delicate information over the system pipe. It will limit the man-in-the-middle attack and spying. SSL is the standard security innovation for setting up an encoded interface between a web server and a program.

This ensures the information go between the server and browser or server and server remains private and not modified by providing encryption and trust Encryption utilizes a private key/open key pair which guarantees that the information can be encoded by one key however must be decoded by the other key . This is referred to as the public-key infrastructure (PKI). Public key is shared while the private key is kept locally.

This is explain in one and two way SSL concerning the files and which are stored where. This is also can be extend to the server to server communication, in addition to the browser to server communication. Trust is gained through the use of certificate. Certificate can be thought as a chain that starts with the certificate authority[18] (or CA).

A Certificate Authority is a company that issues SSL certificates. Web browsers and frameworks come stacked with a list of recognized issuers and that list is kept up to date by automatic updates. Certificates can be self-signed for testing.

Transport layer security (TLS) , secure sockets layer (SSL), are both cryptographic protocols intended to give communication security over a network. The terms SSL and TLS are frequently utilized conversely or in conjunction with each other (TLS/SSL), however one is in certainty the antecedent of the other — SSL 3.0 served as the basis for TLS 1.0 which, as a result, is sometimes referred to as SSL 3.1. In this document, the US government describes TLS guidelines for implementation and indicates that SSL v3 not be used for sensitive government communications or for HIPAA-compliant communications. This graph makes a decent showing with regards to with SSL/TLS support in browsers and the affected vulnerabilities (beast, poodle, crime, rc4).

In two-way SSL, the SSL client device verifies the identity of the SSL server, and then the SSL server application verifies the identity of the SSL-client . Two-way SSL authentication is also known as mutual authentication in light of the fact that the application going about as a SSL customer introduces its declaration to the SSL server after the SSL server validates itself to the SSL client.

## METHODOLOGY

### SSL authentication

SSL authentication and mutual SSL[11,12] authentication also informally known as 1-way SSL authentication and 2-way SSL authentication, respectively. as a developer, if you're interested in developing or be able to debug the mutual SSL authentication effectively, it can be very useful to understand the intricacies of the handshake messages happening under the hood.

SSL authentication, the client is presented with a server's certificate, the client computer might try to match the servers CA against the client's list of trusted car. if the issuing CA is trusted, the client will verify that the certificate is authentic and has not been tampered with. in this aspect, both client, and server use 9 handshake messages to establish the encrypted channel prior to message exchanging.

1. The client sends client hello message proposing SSL options.
2. Server responds with server hello message selecting the SSL options
3. Server sends certificate message, which contains the server's certificate

4. Server concludes its part of the negotiation with server hello done message.
5. Client sends session key information (encrypted with server's public key) in client key exchange message
6. the client sends change cipher spec message to activate the negotiated options for all future messages it will send.
7. The client sends a finished message to let the server check the newly activated options. The server sends change cipher spec message to activate the negotiated options for all future messages it will send.
8. The server sends a finished message to let the client check the newly activated options.

**HTTPS handshake**

Basic SSL Handshake Generally as follows:

1. the client sends the client hello: contains a random number, Session ID, and cipher suite list.
2. The server sends the server hello: contains a random number, Session ID, and session cipher suite.
3. The server sends its certificate: contains server information, Server public key, and hash signature.
4. The server sends the server hello done.
5. The client sends client key exchange: the client uses the public key of the server to encrypt the premaster.
6. The client sends change cipher spec.
7. The client sends Finished: handshake finish message.
8. The server sends change cipher spec.
9. The server sends FinishedÖ handshake finish message.

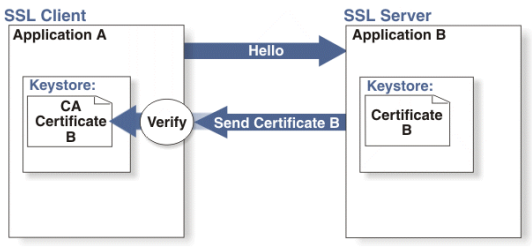


**Fig. 1: SSL Protocol**

**The drawback of SSL and HTTPs protocol**

- **Cost:** It is possible to get a free SSL certificate from a certificate authority, but this isn't recommended. Because free certificate can lack security feature, and cause security issues.
- **Mix Modes:** If mutual SS L authentication isn't setup properly some files can be served as HTTP request rather than HTTPS. Can become a threat to data of visitors.
- **Certification Renew:** SSL certificate should be renewing periodically which add cost to client budget.
- **Proxy Caching:** SSL connections, everything is encrypted including the packet headers and content. Caching that might have happened between the points at which data is encrypted and decrypted is blocked if content is encrypted. Any public caching that might have happened cannot happen. ISPs and others will not be able to cache encrypted content. disadvantages won't affect small to medium-sized sites. It's only the really large sites that might need to think twice about implementing HTTPS.

**SSL Vulnerabilities**

Even though the SSL protocol is used to make data and website more secure, it is vulnerable to many attack security attack[16], some of the are:

- **POODLE Attack:** POODLE stands for **Padding Oracle on Downgraded Legacy Encryption.** It is man-in-the-middle attack[1,2] which exploits clients machine and takes advantage of the internet and security software c fallback client to **SSL 3.0,** which is less secure and easy to decryption. A new version of POODLE attack was announced on December 8, 2014, attack exploits implementation flaws of CBC encryption mode in the SSL protocol. SSL Pulse showed "about 10% of the servers are vulnerable to the POODLE attack against TLS".
- **DROWN Attack: It** stands for "**Decrypting**[13] **RSA with Obsolete and Weakened encryption**". DROWN attack is a serious vulnerability that targets the HTTPS and

services and process rely on TLS or SSL. DROWN allow a hacker to decrypt the client data and stole sensitive data like passwords, credit card number, trade secret or any confidential data from the client computer. A study shows 32**%** of all HTTPS servers are vulnerable to DROWN attack. It allows a hacker to decrypt modern TLS connections between clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.

**Mutual SSL**

Mutual Secure Sockets Layer[17] (SSL) is a cryptographic protocol which provides secure communications for e-commerce, e-mail and other data transfers without eavesdropping, tampering or message forgery.

Mutual SSL has three capabilities that may be used independently or in combination to secure content transport

- **Authenticating** a (web) server to a client (usually a browser).
- **Encrypting** client/server communications.
- **Authenticating** a client to a server.

SSL implementations rely on the user of digital certificates, which verify the identity of people and organizations.

Every certificate contains the following information:

1. Owner's public key.
2. Owner's name or alias.
3. The expiration date of the certificate.
4. A serial number of the certificate.
5. Name of the organization that issued the certificate.
6. The digital signature of the organization that issued the certificate.

**Mutual SSL Authentication**

In mutual SSL[11,12] authentication, both client and server authenticate each other through the digital certificate so that both parties are assured of the others' identity. In this aspect, both client and server use 12 handshake messages to establish the encrypted channel prior to message exchanging.

1. The client sends client hello message proposing SSL options.
2. The server responds with server hello message selecting the SSL options.
3. The server sends Certificate message, which contains the server's certificate.
4. Server requests client's certificate in certificate request message so that the connection can be mutually authenticated.
5. Server concludes its part of the negotiation with server hello done message
6. Client responds with Certificate message, which contains the client's certificate
7. The client sends session key information (encrypted with server's public key) in client key exchange message.
8. The client sends a certificate to verify message to let the server know it owns the sent certificate.
9. The client sends change cipher spec message to activate the negotiated options for all future messages it will send.
10. The client sends a Finished message to let the server check the newly activated options.
11. The server sends change cipher spec message to activate the negotiated options for all future messages it will send.
12. The server sends a Finished message to let the client check the newly activated options.

**Advantages of Mutual SSL protocol**

- **Authentication:** Mutual SSL[11] help to gain customer trust. By authenticating, client

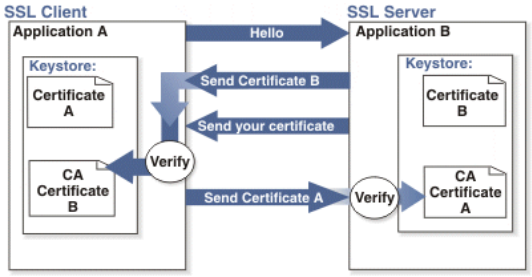


**Fig. 2: Mutual SSL Protocol**

computer sent data to the targeted server not to any unauthorized third party.

- **Protect Against Phishing:** A phishing link redirects the client to an identical copy of the website. Having Mutual SSL help client to authenticate the website and if the client doesn't find connection secure, the client can terminate the connection.
- **Secure:** Mutual SSL uses 256 bit AES algorithm as compare to SSL where it encrypts data using RSA algorithm. Mutual SSL also verifies the server using its digital certificate which provides an extra layer of security to the client machine.

**Implementation**

**1) Mutual SSL Client Server Communication**

In this program , a client-server communication[15] is setup, the output of the project shows the how mutual SSL protocol works and another component like a cipher, hash, key exchange, protocol, certificate: Is Signed, Is Encrypt, a certificate issued to, a certificate[3] issued validity (to-from).

**Output: Server**
**Waiting for a client to connect...**

| | |
|---|---|
| Cipher: | Aes256 strength 256 |
| Hash: | Sha1 strength 160 |
| Key exchange: | 44550 strengths 256 |
| Protocol | Tls |
| Is authenticated | True as a server? True |
| IsSigned | True |
| Is Encrypted | True |
| Certificate revocation list checked: | True |
| | Local cert was issued to CN=localhost and is valid from 06-Feb-12 8:28:50 AM until 01-Jan-40 5:29:59 AM. |
| | Remote cert was issued to CN=localhost and is valid from 06-Feb-12 8:32:08 AM until 01-Jan-40 5:29:59 AM. |

**Output: client**
**Client connected**

| | |
|---|---|
| Cipher: | Aes256 strength 256 |
| Hash: | Sha1 strength 160 |
| Key exchange: | 44550 strengths 256 |
| Protocol | Tls |
| Is authenticated | True as a server? True |
| Is Signed | True |
| Is Encrypted | True |
| Certificate revocation list checked: | True |
| | Local certificate was issued to CN=localhost and is valid from 06-Feb-12 8:28:50 AM until 01-Jan-40 5:29:59 AM. |
| | Remote cert was issued to CN=localhost and is valid from 06-Feb-12 8:32:08 AM until 01-Jan-40 5:29:59 AM. |

## CONCLUSION

This paper presents the performance analysis and working of mutual SSL over SSL protocol[17]. Also, through this research paper, we can conclude that mutual SSL[11,12] is more secure and flexible than SSL protocol. Mutual SSL protocol provides more security than SSL protocol which helps user to preserve sensible information and data on the internet, from a hacker or from another website which use a script to collect the user data from his local machine which lead to privacy breach of the user. By implementing mutual SSL protocol, we can make the web more secure for the normal user as well as for big organizations.

**REFERENCES**


1. Peter Burkholder, "SSL Man-in-the-Middle Attacks", SANS Institute InfoSec Reading, 2003.
2. Michael Howard, "Man-in-the-Middle Attack to the HTTPS Protocol",IEEE computer society, 2009
3. Lakshminarayanan A.1, Jianying Zhou. Flexi Cert: merging X.509 identity certificates and attribute certificates. Proceedings. 14th International Workshop on Database and Expert Systems Applications, 2003.
4. F. Stumpf, "Leveraging attestation techniques for trust establishment in distributed systems," Ph.D. dissertation,Department of Computer Science, Technische Universitat Darmstadt, 2010.
5. Wang K., Fung B. C. M.: Anonymization for Sequential Releases. ACM KDD Conference, 2006.
6. Xiao X., Tao Y. Personalized Privacy Preservation. ACM SIGMOD Conference, 2006.
7. Xiao X., Tao Y. Anatomy: Simple and Effective Privacy Preservation. VLDB Conference, pp. 139-150, 2006.
8. Yao G., Feng D.: A new k-anonymous message transmission protocol. International Workshop on Information Security Applications, 2004.
9. Schoeman, F.D.: Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press. (1984)
10. Parshotam, Rupinder Cheema and Aayush Gulati "Improving the Secure Socket Layer by Modifying the RSA Algorithm" *International Journal of Computer Science, Engineering andApplications* (IJCSEA) **2**, 2012.
11. H. Otrok, R. Haraty, and A. N. El-Kassar,"Improving the Secure Socket Layer Protocol by modifying its Authentication functions" 2006.
12. A. O. Freier, P.Karlton and P.C.Kocher,"The SSL Protocol,version 3.0".
13. C. Jackson, D. R. Simon, D. S. Tan, and A. Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In USEC, 2007.
14. C. Jackson and A. Barth. ForceHTTPS: Protecting high-security web sites from network attacks. In WWW, 2008.
15. Swati Gupta, Saru Dhir ,An Enhanced Approach to Use SSL for End to End Security, Amity School of Engineering and Technology Amity University, Noida.
16. Kefei Cheng, Meng Gao, Ruijie Guo, Analysis and Research on HTTPS Hijacking Attacks, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing.
17. Arthur Goldberg, Robert Buff, Andrew Schmitt Arthur Goldberg, Robert Buff, Andrew Schmitt, A COMPARISON OF HTTP AND HTTPS PERFORMANCE, Computer Science Department Courant Institute of Mathematical Science.
18. LI Wei, XIANG Shuyue, CHEN Shuangbao, Improvement Method of SSL Protocol Identity Authentication based on the Attribute Certificate, International Conference on Computer Science and Service System,2012
19. Norazah Abd Aziz, Nur Izura Udzir and Ramlan Mahmod,Performance Analysis for Extended TLS with Mutual Attestation for Platform Integrity Assurance,IEEE,2014.