Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/103383, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secure Framework to Mitigate Man-in-the-Middle Attack over SSL Protocol

Mohammad Arshad[1] and Md. Ali Hussain[2]

[1]Computer Science and Engineering, KL University, Vaddesewaram – 520002, Andhra Pradesh, India; arshad.klce@gmail.com,
[2]Department of CSE, Andhra Loyola Institute of Engineering and Technology, Vijayawada -520008, Andhra Pradesh, India; alihussain.phd@gmail.com

Abstract

Background/Objectives: Technology has driven the conventional shopping from shop to internet based application tools like PCs, Laptops and smartphones and it is termed as E-Commerce, in which security plays a vital role since it deals with financial transactions. SSL/TLS is responsible for providing security to the application data on both client and server side. **Method:** An overview on E-Commerce security requirements, SLL layer protocol and security analysis of the protocol is conducted. **Findings:** Since E-Commerce services are very important, due to lack of efficient cryptographic encryption techniques, PKI infrastructure and digital signature deployment intruders are intercepting sensitive and valuable information of clients. So we conducted a survey on different attacks on SSL layer of E-Commerce applications and find that Man in the Middle (MitM) attack like phishing attack became a severe attack. **Improvements:** We propose a frame work to mitigate the MitM in SSL protocol which has there modules like front end authentication, backend authentication and bogus CA identification is proposed. Due to dual end authentication its secure compared to traditional SSL. In our future work we implement our proposed framework.

Keywords: E-commerce Security, Man in the Middle (MitM), Public Key Infrastructure (PKI), Secure Socket Layer (SSL), Transport Layer Security (TLS)

1. Introduction

Technology have migrated the traditional shopping to internet based machines like personal computers, laptops and hand held devices like smartphones. E-Commerce applications work over client server phenomena, where customer is client and consumer is server. Security plays a vital role in these applications as it's a matter of financial transactions. Intruders are all the way in between client and server to steal the valuable information like passwords, credit card or banking details.

The whole responsibility of either client and server application data is of Secure Socket Layer (SSL) or Transport Layer Security (TLS). So SSL performs the major operations like mutual authentication between client and server and establish secure and reliable communication channel between them. SSL/TLS is a secure protocol theoretically, but failed practically in real time applications. Researchers have identified vulnerabilities in this protocol recently. Some of well-known attacks are Man in the Middle (MitM) attack Heart bleed attack, poodle attack, cupid attack and many more[1].

Man in the Middle attack is one such type of attack which severely affects the communication channels in between client and server, steals the confidential information and interprets the original data. In this attack

*Author for correspondence

the intruder play a dual role i.e., it appears as a client to server and server to client, intercepts valuable information like public key of both server distributing his own public key for requested one, the both applications on client and server appear to be in secure communication channel.

To secure the SSL/TLS in E-commerce applications new encryption techniques to be proposed which can overcome the existing ones, to establish the secure communication channel between client and server new PKI infrastructure to be designed and the proper technique for digital signature transfer to be proposed. Overall a new framework is needed.

In this paper we propose the secure framework for SSL/TLS for E-commerce applications. Rest of the paper is organized as follows. Firstly we provide an overview of growth and importance of E-Commerce application, secondly discuss about the architecture of SSL/TLS and its vulnerabilities like MitM, and then list out various attacks over SSL/TLS.

2. E-commerce Security

2.1 E-commerce Security Requirements

E-commerce known electronic commerce, which means business trading through internet, both consumers and customers are paying more attention towards E-commerce sites. The main reason for this is successful operations of MNCs like Amazon, eBay, yahoo and many more. Time is more essential in day to day life of human, E-commerce proved its importance by saving customer and consumer time compared to traditional markets. In a fraction of time hundreds and thousands of transaction can be done over e-commerce applications. With a single click customer can perform transaction and consumer can get thousands of transaction with in a small time. Both save time, manpower and transportation. E-commerce can be applied in many real time applications like government sectors (health, finance, industrial, defense and etc.), financial services (banking, investment, finance and mutual funds), Manufacturing, retail, logistics, transport and telecommunication. There are different types of E-commerce with respect to business and customer perspectives, they are i) Business-to-Business (B2B), ii) Business-to-Consumer(B2C), iii) Consumer-to-consumer (C2C) iv) Business-to-Government (B2G)[2].

Security in E-commerce application plays a vital role as it is embedded with financial transactions. Since many third party vendors participate in online shopping transaction there is a chance for theft of confidential and sensitive information. E-commerce applications hold and transfers sensitive and confidential information like passwords and credit/debit card details they need to meet strong security features. The basic security requirements needed by E-commerce application are as below:

- Authentication - Client and server need to prove their original identities.
- Integrity –The third party should not alter the confidential information transmitted between client and server.
- Privacy – No legitimate person can access the confidential information.
- Confidentiality – Only authenticated users can access application data.

In Table 1 we provide the basic security architecture based on OSI reference model. The model demonstrates what measure to be taken at every layer to achieve complete security in E-commerce applications.

2.2 Secure Socket Layer (SSL) Protocol

In[3, 4] authors described that SSL (Secure Sockets Layer (SSL)) is a most popularly used protocol for transferring data between client and server. SSL is a successor of TLS (Transport Layer Security), it operates between application and transport layer of OSI reference model. It acts as an interface between application layer protocol HTTP and transport layer protocol TCP at session layer as shown in Figure 1. SSL is compatible and in build with Netscape, Microsoft browsers and all other web application products. SSL uses both symmetric and asymmetric encryption techniques for mutual transfer of data between client and server, it also uses digital signatures issued by trusted Certificate Authorities. To establish a communication between client and server SSL handshake is established in between them[5] as shown in the Figure 2.

Table 1. Layered security approach for E-commerce application

TCP/IP Layer	Protocol	Security requirement	Security Mechanism	Security Attacks
Application layer	HTTP	Confidentiality, Integrity, Non –repudiation, reliability and anonymity.	Password encryption	SQL Injection attacks, session hijacking, XSS
Transport layer	SSL/TLS, SET	Certification, Digital digest, CA, and Digital signature.	Encryption techniques, PKI.	**MitM**, SYN Flooding, Zero window connection, heart bleed, poodle, cupid
Network Layer	IPV4, IPV6	Content Identity detection, Symmetric encryption, Intrusion detection	Anti – virus, anti- malware, and Firewall	Black hole, Flooding , Resource consumption
Data link layer	IEEE 802.11	---	---	Flooding
Physical layer	----	----	---	Eavesdropping

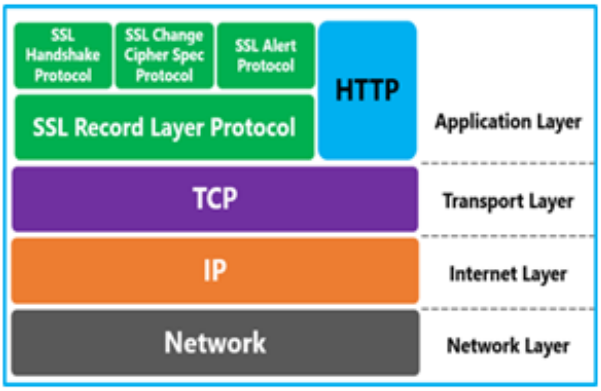

Figure 1. SSL Protocol stack.

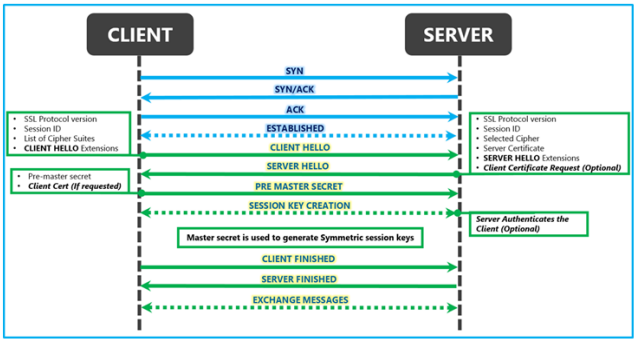

Figure 2. SSL Hand Shake.

2.3 Security Analysis of SSL Protocol

In our analysis we found that SSL is vulnerable to multiple attacks as it is used in all financial transactions like e-commerce payments and mobile transactions. Intruders and hackers can attack SSL/TLS in different ways. Firstly we analyzed different attacks on web applications with respect to OSI layered architecture as shown in below Table 1. Eavesdropping is attack on physical layer which temporarily halts the network services to host. Data link layer is affected with flooding attack where attacker floods too many frames to host. At network layer routing protocol is vulnerabilities like resource consumption, flooding and many more. Application layer and its HTTP and HTTPS protocol is affected with SQL injection attacks.

Session layer which is part of TCP layer is more vulnerable to attacks. SLL is the protocol used at this layer. From literature we have identified some highly affecting attacks over this protocol and they are as.[6-8, 9]

- Man –in- Middle attack.
- Heart Bleed attack.
- Beast attack
- Poodle attack
- Cupid attack
- Attacks against RC4.
- Compression Side channel attacks
- Renegotiation attack
- Attacks against PKI and
- Lack of forward secrecy.

Among the Figure 3. shown attacks Man in middle attack should focused more because it affect over SSL protocol is high.

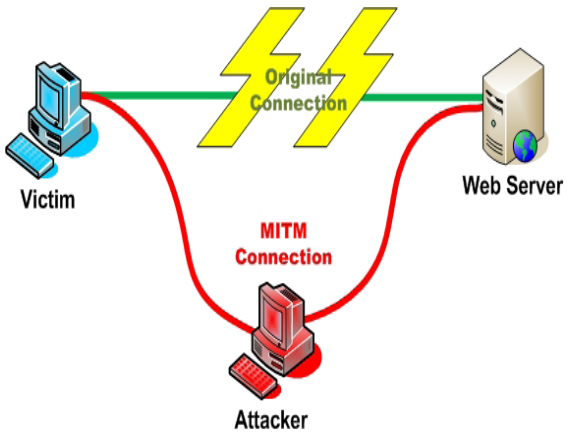

Figure 3. Man in the Middle Attack Model.

2.4 Man – in – Middle Attack Overview

As discussed in early discussion Man-in-the-middle attack[1,5] which intercepts information between client and server secretly. It mainly capture public key of server and its own public key to client, client assumes that it is server public key and sends further information to attacker but not server. A sample of MitM is shown in Figure 2. Where a victim is client and web server is a server which process client request. Using MitM Connection adversary node intercepts confidential information. Though server and client are using proper encryption and decryption algorithms and digital certificates due to some improper authentication techniques they are being exploited to vulnerabilities. Since no additional programs or code like virus, Trojan horse are installed to either sides, it is difficult to find this type of attacks. Antivirus or IDS, IPS can detect this type of attack as it is a external attack but not internal.

There are so many possibilities of implementing man in middle attacks like Address Resolution Protocol (ARP) poisoning, Domain Name System (DNS) Spoofing attack and forged CAs[10]. MitM attacks are very powerful and the attacker plays the role of client in the view of server and vice versa. So the authentication of client with server and server with client is possible for adversary node, all the cryptographic techniques fails here since the client message is bypassed with new message from adversary node and same the server message. The authentication mechanism between client and server fails due to poor authentication techniques against MitM attacks, the main reasons are

1. Due to poor authentication mechanism between Server and client above SSL/TLS.
2. Session established between server and client is based on SSL/TLS authentication.

The above reasons clearly depicts that client is directly communicating with MitM and MitM with server.

3. Proposed Work

Our proposed framework has three modules which are used to perform safe transactions between client device and server. As shown in Figure 4 the modules are as follows:

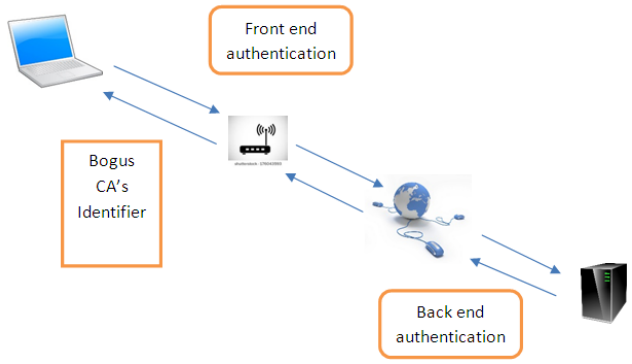

Figure 4. Secure Framework for SSL protocol.

1. Front End Authentication: It deals with client side authentication during client Hello message sent to server. We propose a new encryption scheme which encrypts server public key with state information and of session established between client and server.
2. Back End Authentication: A server side authentication scheme performed during Server Hello message transmission. The same encryption algorithm is used with some modification. Both the authentication mechanisms are used to secure the session[11,12].
3. Bogus CA Identifier: This module will identify the bogus CAs using the novel mechanism that make use of server side database information. Web browser automatically updates its repository with bogus CAs every time they attempt to spoof the client, same done at server side when a server is spoofed.

To make SSL more reliable and secure we want provide back end and front end authentication i.e. back end authentication between web server and Internet service

provider, whereas front end authentication is between ISP and device. Front end authentication mitigate Passive (e.g. hacker in coffee shop or public places) MitM attacks, coming to back end authentication mitigates Active MitM like Secret Agencies like NSA, telecommunication providers. Our frame work is shown in below diagram.

Our framework is more secure since it possess a multi-level authentication and identification of bogus CA. In future work we implement our proposed work and use to mitigate MitM attack on SSL protocol.

4. Conclusion

In this paper we studied about the importance of E-commerce and its security. SSL/TLS layer was effected by most popular attacks like MitM, Heartbleed, and poodle. MitM attack was more over secure socket layer (SSL) or Transport Layer Security (TLS). It is crucial to mitigate this attack, so we proposed a secure framework to mitigate MitM using multiple authentications using state information of session established between client and server and also a technique to identify bogus certificate authorities. In our future work we will implement the proposed framework and compare it with current protocol.

5. References

1. Gangan G , Subodh S .A review of man-in-the-middle attacks.2015.p.1–12.
2. Ismaili E, Houssam H , Houmani H, Madroumi H. A Secure Electronic Payment Protocol Design and Implementation. International Journal of Computer Science and Network Security (IJCSNS) 2015;15(5): 76.
3. Oppliger R . Certification Authorities Under Attack: A Plea for Certificate Legitimation in IEEE Internet Computing. 2014; 18(1):40–7.
4. Meyer C, SomorovskyJ, Weiss E, Schwenk J, Schinzel S, TewsE. Revisiting SSL/TLS implementations: New bleichenbacher side channels and attacks. In 23rd USENIX Security Symposium (USENIX Security2014;14:p.733–748.
5. DasM L,Samdaria N.On the security of SSL/TLS-enabled applications. Applied Computing and Informatics, 2014; 10(1):68–81.
6. Shaik S , Kareemullah K,Hussain M D A . A Study on Network Layer Attacks on MANET Routing ProtocolsNational Conference on Wireless Communications & Sensor Networks. 2014.
7. GujrathiS.Heartbleed bug: Anopenssl heartbeat vulnerability. International Journal of Computer Science and Engineer Science and Engineering.2014; 2(5):61–4.
8. Möller B, Duong T, Kotowicz K. This POODLE bites: exploiting the SSL 3.0 fallback. PDF online.2014.p.1–4.
9. AppeltD, Nguyen CD, BriandLC , Alshahwan N. Automated testing for SQL injection vulnerabilities: an input mutation approach. In Proceedings of the International Symposium on Software Testing and Analysis ACM.2014.p.259–69.
10. Huang L S, Rice A, EllingsenE , Jackson C. Analyzing forged ssl certificates in the wild. In IEEE Symposium on Security and Privacy IEEE.2014. p.83–97.
11. Bhardwaj, Akashdeep et al. Design a Resilient Network Infrastructure Security Policy Framework. Indian Journal of Science and Technology.2016;9(19): 1–8.
12. Magesh S, Nimala K, Meeran A R N. Authentication framework for military applications employing wireless sensor networks and private cloud. Indian Journal of Science and Technology. 2016;9(21):1–6.