Advance Technique for Online Payment Security in E-Commerce : "Double Verification"

Shilpa
Research Scholar
Shri Krishan Institute of Engineering & Technology, Kurukshetra University
Kurukshetra, India
er.shilpa2011@gmail.com

Parveen Sharma
Associate Professor
Department of Computer Science
Shri Krishan Institute of Engineering & Technology, Kurukshetra University
Kurukshetra, India
sharmaparveen19@gmail.com

Abstract— **In E-Commerce various parties involve in E-Payment for buying and selling purpose of goods/services. An Internet E-Commerce Payment Gateway is a critical component for online transaction and that should provide trust to customer that transaction is secure and reliable in all security aspect. There are various vulnerabilities in the present Online Payment system. There is a Man-in-the-Browser attack which is an internet threat/ Trojan horse that can modify web pages and infects web browser and it can also alter transaction content or can add some more data in content. The Trojan can be downloaded or delivered invisibly through Web exploits. This attack is invisible from customer as well as host web application. A MitB attack can take place whether we use SSL, PKI, two or three-factor Security solution. I proposed a advanced technique called "Double Verification" which can detect these MitB attacks while transaction and ensure us secure online transaction over the internet.**

Keywords- Payment Gateway; E-Commerce; SSL(Secure Socket Layer); Double verification; MitB(Man in the Browser); Online payment; Online transaction; TLS (Transport Layer Security)

.1.Introduction

Huge involvement of internet in our day to day life, people feel more comfortable with online transaction in E-Commerce for buying and selling of goods and services .So in this digitalized world people use internet and pay their money electronically. All Online transactions are carried out by the payment gateways which are the access point to financial institutions. Payment gateways authenticate and verify payment detail between various parties and the financial institutions. On that basis it process order as per the customer instruction from merchant website. Security is a major concern in the online transaction system. In Present days there are many open source software like Silent Banker, Paros which can trace your online transaction activity and can alter transaction detail. Now days secure Socket layer (SSL) / Transport Layer Security (TLS) protocol is being used for the secure connection between the client and the server. A lot of research taken over security of SSL/TLS protocol and they all came to same research result as such technologies are vulnerable to different attacks like MitB etc.

2. CONTRIBUTIONS

On the basis of proposed Double/Dual verification system architecture of online transaction, it is possible to do hassle free, secure and reliable online transaction. I design and develop this architecture for secure online transaction.

3. EXISTING SCENARIO

In existing system online transaction system works with the payment gateway with SSL/TLS. Payment gateway act as a bridge between merchant application host server to bank server and data transferred from merchant application host server to bank server is in encrypted format by using SSL.

According to Ved Prakash Gulati [2], when an online transaction takes place these function comes in the picture Authorizing, Clearing and Reporting. As firstly when customer wants to buy a product so customer will click to buy .If merchant website has SSL certificate then there visitor get know that entering their personal information over the website will be safe and transactions will also be secure. It can be identified by an https prefix (display in browser address bar) which ensures website is protected. The SSL certificate will be issued to encrypt data transfers like customer bank details and to identify that merchant website has matching information on file with the CA. The encrypted data send via payment gateway to bank server where data is decrypted and authenticate (customer detail with bank) transaction details and then bank will give response after validating and depending upon the credit limit, bank will reject or accept the transaction. After this payment gateway then transmits the receipt of bank to the merchant website as report.

3.1 Existing Online Payment Transaction Technique for Security:

According to Holly Lynne McKinley [1], Existing Online Payment transaction communication is secured by using SSL/TLS protocol in order to protect the connection between the customer and the server. However, SSL/TLS protocol is vulnerable to different attacks.

SSL communication follows following steps:

Step 1. Establish Secure Communication:

Customer send https request, the SSL layer initiates a communication handshake channel.

Step 2. The SSL Handshake Channel:

a. The customer's web browser sends the Bank website server its methods of encrypting data with other information like encryption type and other SSL related data.

b. The Server provide its own data like SSL certificate with public key, it is used for encryption as well as other secure sockets layer information.

c. The customer's browser checks the received information like certificate expiration date and valid certificate authority.

Step 3. Completing the SSL Handshake:

a. Now browser creates a "premaster secret" that will be used to encrypt the data for entire session. “Premaster Secret” is a random key that it encrypts using the agreed upon encryption method combined with the server's public key string that it received and sends the new encrypted secret string back to the server.[9]

b. With the new "premaster secret" string, the browser and the web site server create a new "master secret" string and use it to create session keys (long characters strings) that their encryption programs use for the rest of the session to encrypt/decrypt all transmissions . Using Master secret key browser and server both are able to verify that the data did not change in network transmission.

c. Now browser sends a message as start secure communication by using new session key.

d. The web server send back ok response to browser as start secure communication by using new session key.

e. The web server (encrypted communication) verifies to the browser that it is finished securing its part of the session.

The browser and the web server use the session keys to encrypt and decrypt the data they send to each other.

Existing online transaction systems assume that above SSL steps provide online security for online transaction. But According to Peter Burkholder [3], this secured communication channel has also vulnerability of attacks.

4. PROPOSED TECHNIQUE (ONLINE PAYMENT TECHNIQUE WITH DOUBLE VERIFICATION):

When a customer wants to buy a product from E-commerce website, customer wish to do online payment for it. So to make online payments customer has to interact with Payment Gateway. Through the payment gateway customer selects the bank through which he has to do payment for merchant website from which customer buying a product.

In Online Payment Transaction there are two types of communication takes place. First two communications exists in existing techniques. Third communication is evolved for verification in my proposed technique in which double verification technique is initiated.

1. Communication Between Customer Browser to Merchant website

2. Communication Between Customer Browser to Bank Server
3. Communication Between Bank Server to Merchant Server (Double Verification)

It is possible to hack / tamper /alter the payment request in first two communication mentioned above. So as to avoid this one new concept called Double Verification is evolved.

Basically in online transaction security these are the parameters which are used.

- Transaction Id – Generated by the merchant when transaction initialize.
- Merchant Code – Decide by the payment gateway provider/bank for each merchant.
- Amount- Payment money.
- Reference Number – Bank generated Id after payment.
- Transaction Status – It has two values “Success” or “Failure”.

4.1 Following are the Steps of a Secure Online Transaction:-

1. Customer visits to merchant website on PC browser, Authentic through Username/Password/DSC etc then select a product and choose a payment option to proceed for online payment.
2. Now a request string (contains transaction id, reference id, amount) is being prepared in clear text which is converted into an encrypted string using a symmetric key which will be provided by Bank. Bank provide key for each merchant which contain merchant code along with encryption algorithms.
3. This encrypted string forwarded to Bank and Bank decrypt (using same shared key) it & checks its validity, ask User name and password from user and after processing send the response back to Merchant server not on the Customer browser.
4. Now initialize double verification process as Merchant application servers again send an encrypted request string for enquiry of this transaction using Merchant Unique Reference number.
5. Bank server receive the encrypted request and after decryption of request string data using shared key it fetches data against provided Reference number from its database then send back encrypted response of this enquiry to merchant server.
6. Now Merchant receive the response after decryption of encrypted response it compare the Bank Transaction ID Amount and Status received in the Step (3) and received in the Step (5), if both are equal then only this transaction is being treated as Success. In all other cases it is being treated as failed transactions.

4.2 What was the Problem Earlier before Double Verification Functionality?

Traditionally Online Payment Transactions did not have third communication channel mentioned above, so it is possible to tamper/alter the online payment request using freeware tools like Paros. Hacker can alter the Amount e.g. Rs. 10000 to Rs. 1 and forwarded to Bank and while response was coming back to Customer Browser before landing on browser Amount again altered from Rs 1 to Rs. 10000. As this request response was going on Customers browser Merchant website was not aware about the Man in Middle attack.

4.3 How above problems got resolved?

1. **Converting Clear Request String to Encrypted Request String:** - Traditionally all request string was sent to bank in Clear text and visible to a non technical person in the Address bar of browser. So first it is required to change this clear text to Encrypted. For this feature bank can provide a unique symmetric key for each merchant code by which all the request string being encrypted before sending it to Bank. This key can be stored on server of Bank and Merchant in safe manner.
2. **Using Double Verification Request String:** - Even after incorporation of encrypted string to make this process more robust, functionality is developed in my proposed technique to verify the response received from bank which is called Double Verification. Objective of double verification is to enquire from bank what is the status, Amount and transaction ID at bank side for the initiated transaction. On receipt of the response from bank both the response (First response before Double verification and second response after Double verification) received is being compared for it validity. So that we can check payment transaction was tempered/altered or not. If in any case transaction data was tempered at any point it will give status “fail”.

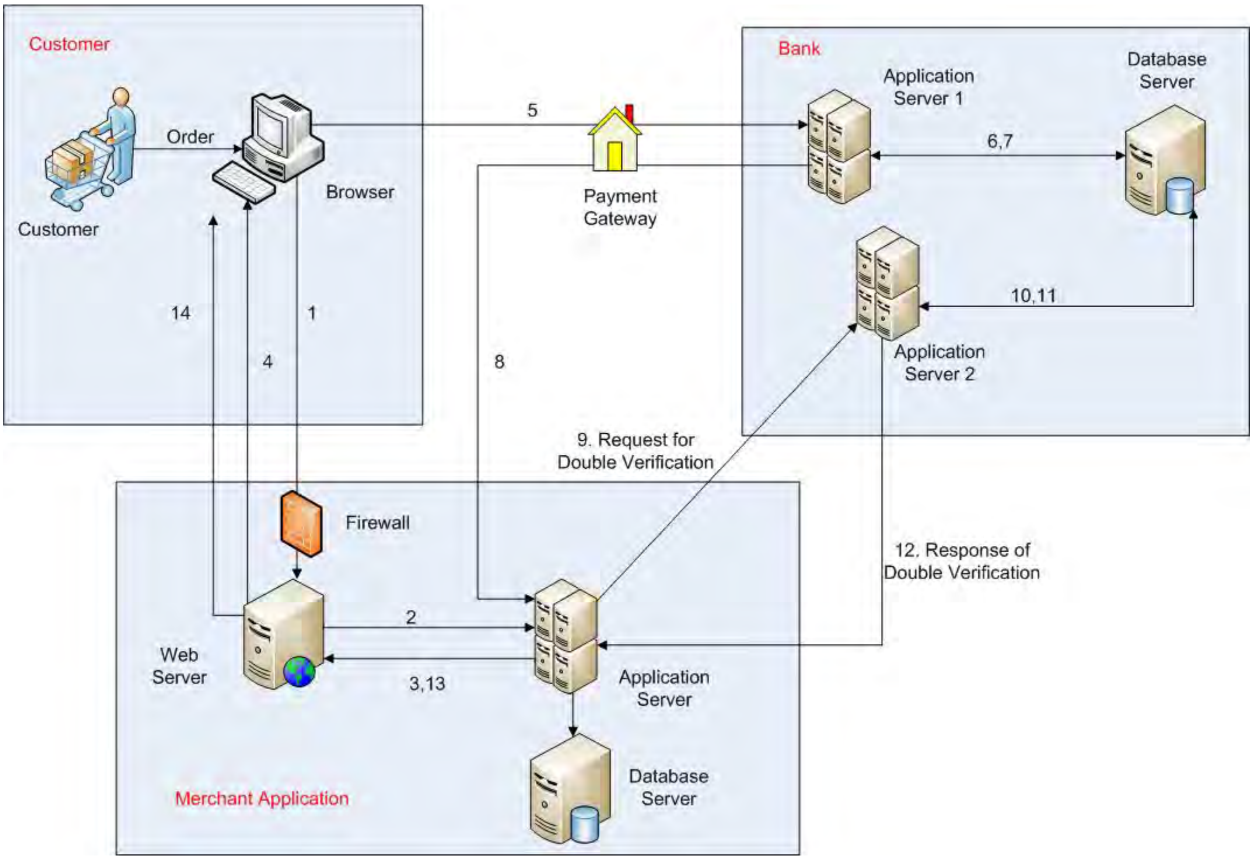

Figure 1 Double Verification Technique in Online Payments

Detail Description of Fig. 1 (In Figure number indicate respective Steps)

Step 1: Customer visits to the merchant website and after selection of payment option for the product which customer wants to buy, and then request goes to the Merchant web server.

Step 2: Merchant web server receive the request and send request to application server.

Step 3: When Merchant application server receive a new payment request .It will generate a transaction id value and insert this transaction id value along with null status to database against the visiting customer. And send back response to web server.

Step 4: Merchant web server receive the response and send encrypted response to the web browser.

Step 5: Now a request string (contains transaction id, amount, customer detail) is being prepared in clear text which is converted into an encrypted string using a symmetric key provided by Bank which is unique for each merchant.

Step 6: Bank application servers receive encrypted data and decrypt data using symmetric key and after check customer credentials with bank database and after successful verification of customer credentials, as per customer instruction bank server debit/credit customer money bank generate a Reference number against that transaction.

Step 7: Bank Database server save the transaction Id, reference number amount along with status into database and also send back data to bank application server.

Step 8: Bank application server send encrypted transaction detail (transaction id, reference number, status, and amount) response to the Merchant application server.

Step 9: Double Verification Initiation :- Merchant application server immediately initialize the request of double verification after getting first response ,it send the encrypted request data which contains (transaction id, reference number, status, and amount) to bank application server.

Step 10: Bank application server receives the encrypted request and decrypts the request using symmetric encryption. Send enquiry to database server to get reference number corresponding detail.

Step 11: Bank Database server provide the transaction detail corresponding the reference number to the bank application server.

Step 12: Bank application server send encrypted response to the merchant application server which contains the transaction detail .If Step 8 response is same as this response then it means transaction is “Successful” else online payment data is tempered /altered i.e. if both response is not matched then it will means online payment is “Failed”.

Step 13: Transaction status send to Merchant web server.

Step 14: Merchant web server receive the response and send response to the web browser for display to customer.

5.DOUBLE VERIFICATION ALGORITHM:

We know that online transaction carried out by the payment gateway which has customer, Bank, Merchant as entity. Each entity play an important role in online transaction and also follows protocols /algorithms .But in this paper my main concern is online double verification process which follow server (merchant) to server (bank Server) communication.

Double Verification algorithm:

Merchant Server	Bank Server
Step1: Merchant has Reference Number, transaction Id and amount. Step 2: Encrypt data string using key. Step 3: Incorporate parameter to link (link should be provided by bank). Step 4: Create merchant server to bank server connection. Connection established on a specific port which is assigned by bank. Step 5: Send encrypted code to Bank server. Step 6: Get response which include transaction status, amount etc. from Bank server. Step 7: Compare given amount (Step 1 amount) to retrieved amount (Step 6). If amount is same then return status “Success” else “Failure”.	Step 1: Get encrypted code from merchant host server Step 2: Decrypt it using shared key and get transaction id, reference id, merchant code, and amount. Step 3: Bank creates connection with its database. Step 4: Check details for given reference number in its database. Step 5: Retrieve transaction amount against ref no encrypt the result and Send back response to merchant server.

6. CONCLUSION

In this paper, I give a Double verification technique in online transaction to do hassle free payment over the internet .This technique use server to server communication without known to user .We see in this paper how double verification can hold security measure for secure online payment.Using Double Verification technique we can detect Man in the Browser attack and other attacks which alter data while transmission of data over the network and ensure online payment is trusted in E-Commerce.

7.REFERENCES

[1] Holly Lynne McKinley,”SSL and TLS: A Beginners”, SANS Institute 2003,Guide-,GSEC Practical v.1.4b
[2] Ved Prakash Gulati And Shilpa Srivastava – “The Empowered Internet Payment Gateway”
[3] Peter Burkholder, “SSL Man-in-the-Middle Attacks”, SANS Institute,February 1, 2002 (v2.0)
[4] Yang Jing ,“On-line Payment and Security of E-commerce”, ISBN 978-952-5726-00-8 (Print), Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09), Nanchang, P. R. China,, pp. 046-050, May 22-24, 2009
[5] Pradeep Kumar Panwar, Devendra Kumar -“Security through SSL” -Volume 2, 2012, IJARCSSE, Issue 12, ISSN: 2277 128X In,December 2012.
[6] Elmo Todurov- “SSL, man-in-the-middle attacks and root CA’s” -Institute of Cybernetics, Tallinn- January 24,2013 .
[7] Rossilawati Sulaiman, Dharmendra Sharma, Wanli Ma, and Dat Tran – “Securing Online Communications using MLC and MAS in E-Health”, Australian Journal of Basic and Applied Sciences-, 6(9): 588-604, 2012.
[8] Stephen A. Thomas-“ SSL and TLS Essentials: Securing the Web” 5/25/2001 EDT
[9] “ How does ssl work?” http://www.ourshop.com/resources/ssl_step3.html-2011.
[10] Artur Salagean- “The technologies used in security in online payments”, Web Coder -2012.

8.AUTHORS PROFILE

Shilpa is Research Scholar in Shri Krishan Institute of Engineering & Technology affiliated to Kurukshetra University, Kurukshetra. Her technical interests include research, banking, banking technology, E-Governance, and E-procurement.

Parveen Sharma is Associate Professor & head of Computer Science department in Shri Krishan Institute of Engineering & Technology affiliated to Kurukshetra University, Kurukshetra.