A Simulation Test Based on Improved SSL Protocol

Xueqin Huang[1], Geng Qiang[2,*]

[1]Department of Information, Hainan College of Economics and Business1, Haikou, 571127, China
[2,*]School of Information Engineering, Haikou College of Economics2, Haikou, 571127, China

***Abstract*—Through the safety analysis of SSL operation in the current flow of online payment, the defect of identity authentication of SSL protocol in the application of e-commerce is identified and an improved protocol strategy is proposed. The online payment model is improved based on the improved SSL protocol and the online payment flow is shown within the improved model. LoadRunner is applied for simulation comparison to prove the improved SSL protocol could run normally with non-repudiation.**

Keywords-e-commerce; online payment; SSL protocol; digital signature; loadrunner.

I. INTRODUCTION

In recent years, along with the continual development of computer network technology, e-commerce application has been greatly advanced. However, various information safety problems occur repeatedly along with it and the safety problem concerning online payment is one of them.

At present, the safety protocols for online payment mainly include Secure Sockets Layer protocol. Although it can provide many functions of identity authentication, data security and information integrity in electronic payment, SSL protocol has many limits in which the chief one is SSL protocol has no function of digital signature without non-repudiation. For this defect the thesis provides improvement strategy and carries out software simulation comparison to prove that improved protocol could run normally with non-repudiation.

II. ANALYSIS OF TRADITIONAL ONLINE PAYMENT FLOW

A. Construct an online payment simulation platform

In order to show more clearly the SSL execution flow in online payment, a basic online payment operation model is designed. InFig.1 e-commerce website is published at WWW server end (Install Windows Server 2003) and the “Certificate Authority” module is installed in another server to simulate a certificate authority (CA) as shown in Fig.1.

Meanwhile the module of “Safety Communication” in “Catalog Safety” service is configured for the WWW server. That means WWW server applies for safety authentication at CA and then award certificate to WWW server, and after installation of the certificate WWW server may provide SSL safety certificate service and thus construct a SSL protocol-based online payment environment.

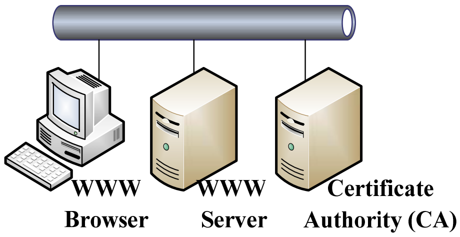


Figure 1. Basic topological structure

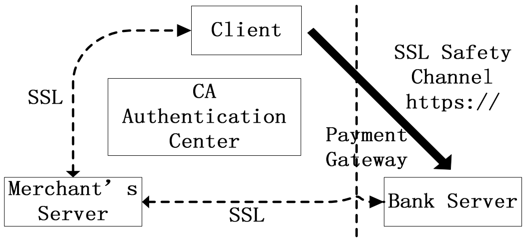


Figure 2. Traditional SSL-based model

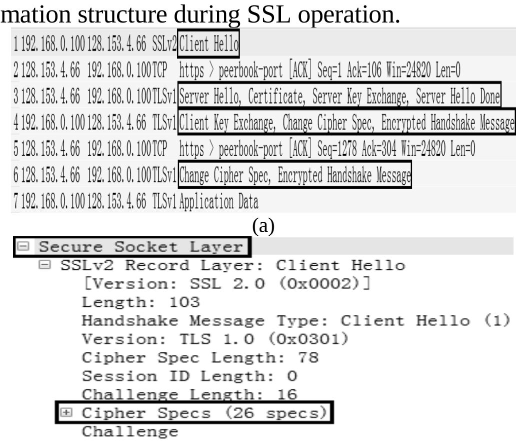
Fig.2 shows a traditional SSL protocol-based online payment flow: 1.the client applies for online bank account and download certificate; 2.the client visits merchant’s website, browses related goods, fills in purchasing order information and sends to merchant and meanwhile verifies merchant’s identity; 3. after receiving the order merchant replies to the client, the browser at client’s end pops up prompt to establish a new page of safety connection with the selected bank. Then the client end is going to link with bank server and SSL protocol mechanism is involved. The client end will automatically verify the digital certificate of bank server and SSL handshake protocol is completed and a safety channel is established between the two sides; 4. the client fills in payment information in the payment webpage of bank and the page will show the corresponding order and payment amount information from the merchant for affirmation. After the payment, the client will confirm and end safety SSL connection; 5. the bank carries out fund settlement in backstage with merchant’s opening bank and shift related fund to merchant’s account and send successful payment information to the merchant[1,3]; 6. after receiving the successful payment information of the client from bank, the merchant will send receipt confirmation to the client and finish the payment.

B. *Analysis of SSL protocol flow by capture package*

SSL protocol is situated between TCP/IP protocol and application protocol in two layers. The upper layer in TCP is SSL recording protocol which provides basic functions like data encapsulation, compressing, encryption and others; another is SSL handshake protocol which is to carry out identity authentication for both sides of communication, negotiation of encryption algorithm and exchange of secret key before data transmission.

At this moment the merchant's WWW server may be visited through WWW browser at the client's end. SSL protocol is involved in information exchange and Wireshark may be installed at WWW server for packet capturing in communication. Data interaction is shown in Fig.3. After data package filter operation, data no. 1 will be sent from the client's end (192.168.0.100) to the server's end (128.153.4.66) by SSL protocol， and the report structure is shown as follows after selection.

It can be shown that the client's end sends Client Hello information to the server's end including client-supported encryption algorithm, random number, version number, dialogue ID, acceptable Cipher Spec and compression method, etc. The chosen box in Fig.3 shows the key information structure during SSL operation.



```
1 192.168.0.100 128.153.4.66  SSLv2  Client Hello
2 128.153.4.66  192.168.0.100 TCP    https > peerbook-port [ACK] Seq=1 Ack=106 Win=24820 Len=0
3 128.153.4.66  192.168.0.100 TLSv1  Server Hello, Certificate, Server Key Exchange, Server Hello Done
4 192.168.0.100 128.153.4.66  TLSv1  Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5 128.153.4.66  192.168.0.100 TCP    https > peerbook-port [ACK] Seq=1278 Ack=304 Win=24820 Len=0
6 128.153.4.66  192.168.0.100 TLSv1  Change Cipher Spec, Encrypted Handshake Message
7 192.168.0.100 128.153.4.66  TLSv1  Application Data
```

(a)

```
⊟ Secure Socket Layer
  ⊟ SSLv2 Record Layer: Client Hello
      [Version: SSL 2.0 (0x0002)]
      Length: 103
      Handshake Message Type: Client Hello (1)
      Version: TLS 1.0 (0x0301)
      Cipher Spec Length: 78
      Session ID Length: 0
      Challenge Length: 16
    ⊞ Cipher Specs (26 specs)
      Challenge
```

(b)

Figure 3. SSL protocol capture package

The handshake protocol interaction process between SSL protocol client and the server shown in the captured record is shown in Fig.4.

Judging from the handshake process of SSL protocol, it only provides identification for browser and server rather than identity authentication for clients and merchants. Therefore once the two parties propose objection after transaction, SSL protocol cannot provide complete non-repudiation function and there exists defect of identity authentication [4].

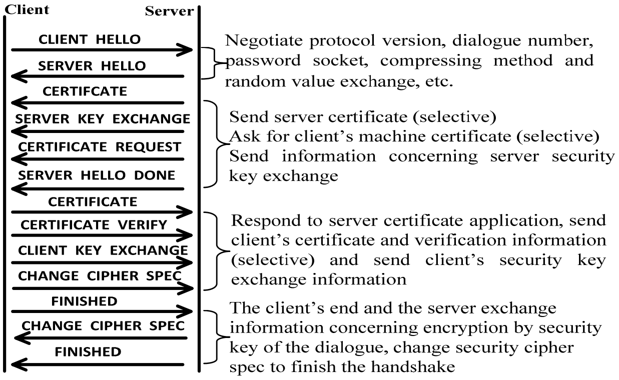
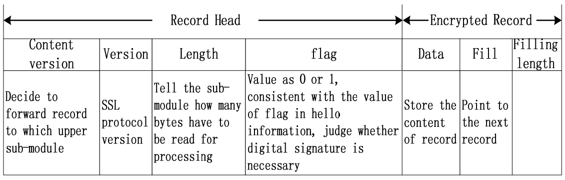

Client
Server
CLIENT HELLO
SERVER HELLO
CERTIFCATE
SERVER KEY EXCHANGE
CERTIFICATE REQUEST
SERVER HELLO DONE
CERTIFICATE
CERTIFICATE VERIFY
CLIENT KEY EXCHANGE
CHANGE CIPHER SPEC
FINISHED
CHANGE CIPHER SPEC
FINISHED
Negotiate protocol version, dialogue number, password socket, compressing method and random value exchange, etc.
Send server certificate (selective)
Ask for client's machine certificate (selective)
Send information concerning server security key exchange
Respond to server certificate application, send client's certificate and verification information (selective) and send client's security key exchange information
The client's end and the server exchange information concerning encryption by security key of the dialogue, change security cipher spec to finish the handshake

Figure 4. SSL handshake protocol flow

III. SSL PROTOCOL IMPROVEMENT IDEAS

To sum up, since SSL provides no digital signature for application layer, transaction non-repudiation and identity authentication is not provided. It can be improved in the following ways:

At first add a flag in the data of Client Hello and Server Hello in SSL handshake protocol to show whether the opposite side is necessary to carry out digital signature for the information； meanwhile also add a flag in recording protocol with the value consistent with the flag of Client Hello and Server Hello with the structure shown in Fig.5; and then modify Certificate Request at server end and Client Certificate at client's end, when there is digital signature demand, Certificate Request at server end is compulsory, after the client's end receives Certificate Request from the server, if there is related certificate, it will send a Client Certificate to the server, and after verification the server will continue the communication; otherwise it will send no Certificate to the server, since the server asks for digital signature, the server will declare the handshake fails.



Record Head				Encrypted Record		
Content version	Version	Length	flag	Data	Fill	Filling length
Decide to forward record to which upper sub-module	SSL protocol version	Tell the sub-module how many bytes have to be read for processing	Value as 0 or 1, consistent with the value of flag in hello information, judge whether digital signature is necessary	Store the content of record	Point to the next record	

Figure 5. Improved SSL recording format

When SSL records data sent by the protocol from the upper layer, first check the flag. If the flag is 1, divide the data into segments, and get MAC after calculating, and add MAC to the end of data slot. Encrypt MAC with private key to form digital signature to replace the MAC before encryption and put it at the end of data slot, and then encrypt the whole data slot (including data segments and encrypted MAC) with encryption algorithm to form encrypted load and add record head information [2]. Finally data will be sent by TCP linkage as shown in Fig.6. If flag is 0, carry out data transmission in traditional manner.

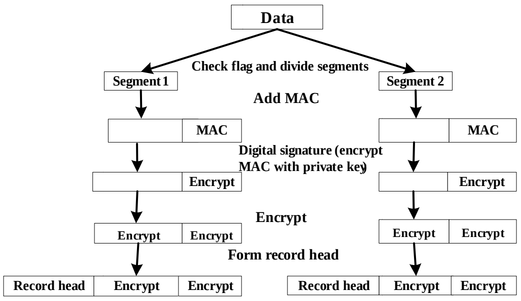


Figure 6. Record forming process with Flag as 1

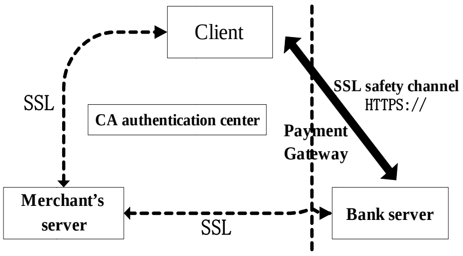


Figure 7. Improved SSL protocol model

IV. ONLINE PAYMENT FLOW BASED ON IMPROVED SSL PROTOCOL

The improved SSL protocol online payment flow mainly improves step 3 of traditional flow: the browser at client's end pops up prompt to establish a new page of safety connection with bank server. When the client end is going to link with bank server, SSL protocol mechanism is involved. The client end will negotiate with bank as to whether digital signature is necessary and the client will automatically verify the digital certificate of bank server while the server will select whether to verify the digital signature of the client's end according to the negotiation. If the negotiation asks for digital signature, bank will verify the digital certificate of the data and after verification [5], SSL handshake protocol is completed and a safety channel is established between the two sides as shown in Fig.7.

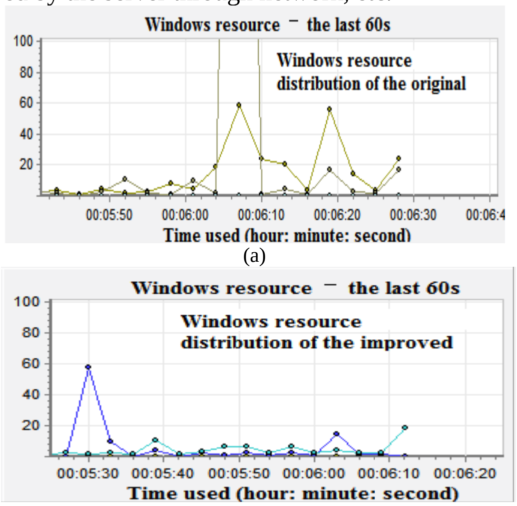
V. ONLINE PAYMENT SIMULATION TEST BASED ON IMPROVED PROTOCOL

LoadRunner is a tool developed by HP which can simulate many users, carry out concurrence load real-time performance supervision to predict system action as well as evaluate system performance.

A. Online payment system response test under two protocols

The simulation is designed as 100 Vuser visit Web server sites through SSL encrypted linkage. Visitors are increased in a gradual manner, i.e. two users are initiated every 15s, and when visiting stops visitors are reduced gradually, i.e. 5 users every 30s so as to simulate the visiting mode of real users to the greatest extent.

As shown in Fig.8, in the simulated period, for the two protocols, in terms of Windows resource distribution, along with the increase of users, occupied Windows resource stays around 20% with the maximum peak within 60% with no distinct difference. Windows resource parameters selected mainly include number of webpage errors in processor, the percentage of time used for the chosen disk drive to deal with reading or writing demand, number of bytes sent and received by the server through network, etc.

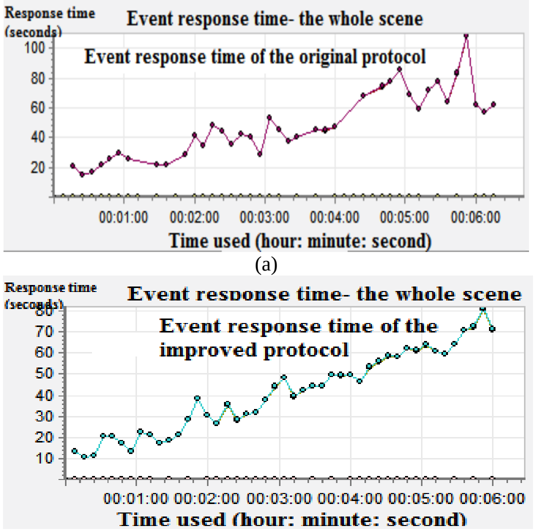


(a)

(b)

Figure 8. Contrast of server resource occupying time of two kinds of protocols

Fig.9 shows during the simulated period, for the two protocols, along with the increase of users, the response time for online payment events also increases gradually without big fluctuation and the event response time for the two protocols stays roughly the same.



(a)

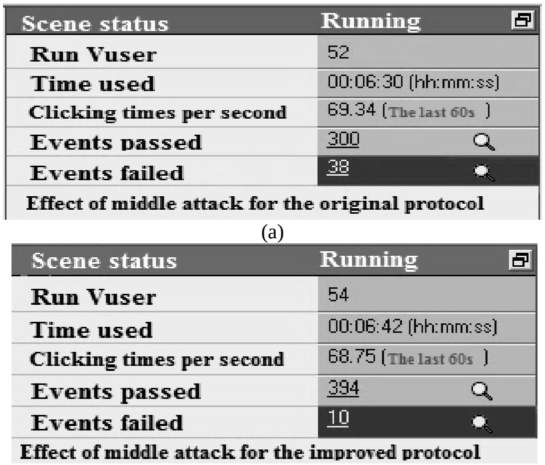
(b)

Figure 9. Contrast of response time of two kinds of protocol servers

The simulation proves that the improved SSL online payment mode, since only a CA authentication process is added in the added digital signature, little effect is made for system resource and system event response and thus proves that the improved protocol has not damaged user experience with good operability while improved safety.

B. Identity authentication validity test under two protocols

Cain & Abel network attack software is applied to simulate the middle attack for SSL protocol. When LoadRunner is used to record simulation script attack is made and monitor event treatment scheme like normal online payment between user and website, as shown in Fig.10.



Scene status	Running
Run Vuser	52
Time used	00:06:30 (hh:mm:ss)
Clicking times per second	69.34 (The last 60s)
Events passed	300
Events failed	38

Effect of middle attack for the original protocol

(a)

Scene status	Running
Run Vuser	54
Time used	00:06:42 (hh:mm:ss)
Clicking times per second	68.75 (The last 60s)
Events passed	394
Events failed	10

Effect of middle attack for the improved protocol

(b)

Figure 10. Effect of middle attack for the two kinds of protocols

Through the simulation, it can be shown that during the middle attack, since the improved protocol added the function of digital signature, middle attack becomes more difficult, thus under the improved protocol, “the failure” of user’s visit to the serve decreases 28 than the original one which shows the improved SSL protocol has effectively decreased the effect of middle attack and realized user identity authentication.

VI. CONCLUSION

The thesis proposes improvement strategy for SSL protocol-based online payment. Through simulation proves the feasibility of protocol improvement. Therefore compared with traditional model, online payment flow based on the improved protocol can perfect bank’s identity authentication for the client in the interaction between client and bank with no effect for the interaction. Meanwhile digital signature can be applied to identify the user so as to realize the non-repudiation of transaction.

REFERENCES

[1] WU G F, W F F, Z Y. Solutions to two methods of SSL protocol attack [J]. Journal of Hefei University of Technology (Natural Science), 2013; 36(10): 1217-1221.

[2] Zhang X D. The Improvement strategy of the SSL security protocol based on digital signature[J].Journal of Hunan Industry Polytechnic,2009,9(3):14～15,47.

[3] Li L. The Analysis and Comparison of SSL and SET in Electronic Commerce [J]. Netinfo Security, 2011(04).

[4] Zhang Xue, Ma Guangsi, Mao Hong yan. Research of Improving Safety E-Trade Performance Based on SSL [J], Microelectronics Computer, 2011(02).

[5] Chen X Q. Research and improvement of online payment model based on SSL protocol [D].Shenyang: Northeastern University.2012.