ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Noval Approach on Online Transaction Protocols

Ms. Renu *, Ms. Ritu
renusheoran442@gmail.com

Abstract

The increase of wireless devices, offering connectivity and convenience, continues to exert marvelous demands on merchants to deploy secure wireless applications including electronic commerce. Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the protocol above TCP, which can protect user's privacy when they sending data from a client side to a web server, this is an important protocol due to the expansion of Internet. In fact, it is a long way to make the SSL/TLS protocol perfectly. Although the Secure Electronic Transaction (SET) protocol offers end-to-end security for credit card transactions over a wired infrastructure, there are several factors including bandwidth requirements which make it unsuitable for wireless applications. In this paper we review a secure electronic payment system for Internet transaction. The electronic payment system is to be secure for Internet transaction participants such as Payment gateway server, Bank sever and Merchant server. The security architecture of the system is designed by using Many Security Protocols and techniques, which eliminates the fraud that occurs today with stolen credit card/debit card payment information and customer information. Electronic commerce involves the exchange of some form o f money for goods and services over the Internet but today, Internet is an insecure and unreliable media. The asymmetric key cryptosystem The confidential information of customer could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption methods to enhance data security as well as authentication of data communication. The multiple encryption technique provides sufficient security for electronic transactions over wireless network.

Keywords: SSL Protocol, SET Protocol, symmetric & asymmetric Methodology, Dual signatures..

Introduction

The unstable growth in the use of mobile devices is problem-solving of the next computational platform, then consumers will soon have the option of accessing web-based applications using personal computers . This superb growth fueled by consumers' need for mobile access to information and other services, is serving as a catalyst for the development and deployment of secure wireless applications including electronic commerce. Now, many different payment protocols are used to hold electronic payments over the Internet : SSL, E-cash , e-Check, Secure Electronic Transaction (SET) .While these methods of payment do fulfill the customer's needs. Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the protocol above TCP, which can protect user's privacy when they sending data from a client side to a web server, this is an important protocol due to the expansion of Internet. In fact, it is a long way to make the SSL/TLS protocol perfectly Whereas an effort to standardize credit card payments through SET has proved beneficial, standards do not necessarily exist for the remaining types of payments. Later, any attempt to migrate these payment protocols from the wired to the wireless environment will more than likely result in a similar excess of protocols.

What will prove valuable is a standard payment protocol that supports both credit and debit card payments over wireless networks in a secure and efficient manner. The Secure Electronic Transaction is an open encryption and security specification planned to protect credit card transactions on the Internet. The companies that collaborated in the development of SET include IBM, Microsoft, Netscape, RSA, Terisa and Verisign. It is supported by major corporations such as VISA Inc. and MasterCard. Even though SET have been designed to operate in a wired infrastructure , its transaction flow and implementation of security are of interest to us since it can also be employed in a wireless scenario.

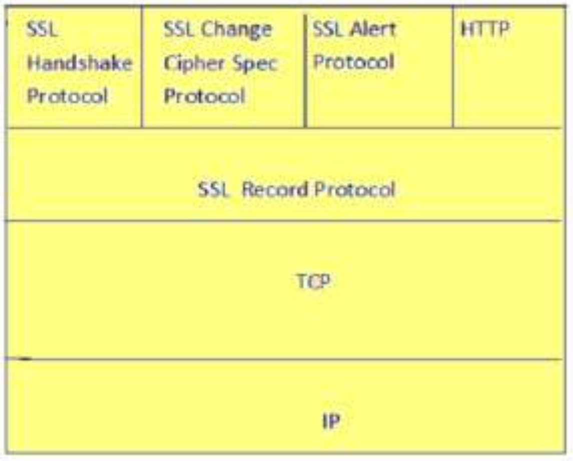
The SET protocol is a progress of the existing credit-card based payment system that provides enhanced security to transfer informatons as well as authentication of transaction participant identities by registration and certification. SET is also an international standard with published protocol specifications. While SET permits customers to make credit-card payment to any merchant offering web-based services, customers also have the option of paying for other types of services using the on-line banking facilities.

A. Secure Socket Layer(SSL)

SSL supports the Diffie-Hellman protocol, the majority of SSL transactions use the RSA public key algorithm to distribute secret-key parameters, they do not use public-key agreement approach.

SSL is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL Connection. Both Netscape Navigator and Internet Explorer support SSL and many Web sites use the protocol to safely transmit confidential information, such as credit card numbers. A number of approaches to providing Web security are possible. The various approaches are similar in many ways but may differ with respect to their scope of applicability and relative location within the TCP/IP protocol stack. For example we can have security at the IP level making it transparent to end users and applications. However another relatively general-purpose solution is to implement security just above TCP. The primary example of this approach is the Secure Sockets Layer (SSL) [1]. The Secure Sockets Layer (SSL) provides security for web based applications. It uses s TCP to provide end –to-end secure services.SSL is not a single protocol but rather two layers of protocols. It can be seen that one layer makes use of TCP directly. This layer is known as the SSL Record Protocol and it provides basic security services to various higher layer protocols. An independent protocol that makes use of the record protocol is the Hypertext Markup Language (HTTP) protocol. Another three higher level protocols that also make use of this layer are part of the SSL stack. They are used in the management of SSL exchanges and are as follows : 1. Handshake Protocol. 2. Change Cipher Spec Protocol. 3. Alert Protocol.

Figure:



A. SSL Record Protocol

This protocol provides two services for SSL connections: 1. Confidentiality - using conventional encryption. 2. Message Authentication - using a Message Authentication Code (MAC).

1) Confidentiality: ***eavesdropping:*** The SSL protocol encrypts all application-layer data with a cipher and short-term session key negotiated by the handshake protocol. A wide variety of strong algorithms used in standard modes is available to suit local preferences; reasonable applications should be able to find an encryption algorithm meeting the required level of security. Key-management is handled well: short-term session keys are generated by hashing random per connection salts and a strong shared secret. Independent keys are used for each direction of a connection as well as for each different instance of a connection. SSL will provide a lot of known plaintext to the eavesdropper, but there seems to be no better alternative; since the encryption algorithm is required to be strong against known-plaintext attacks [2]

2) Confidentiality: traffic analysis: The Secure Socket Layer was introduced primarily to provide private web access. HTTP requests and replies are encrypted and authenticated between clients and servers, to prevent information from leaking out. When the standard attacks fail, a cryptanalyst will turn to more obscure ones. Though often maligned, traffic analysis is another passive attack worth considering. Traffic analysis aims to recover confidential information about protection sessions by examining unencrypted packet fields and unprotected packet attributes. There are some more understated threats posed by traffic analysis in the SSL architecture.

Bennet Yee has noted that examination of cipher text lengths can make known information about URL requests in SSL. SSL includes support for casual filling for the block cipher modes, but not for the stream cipher modes. We believe that SSL should at the minimum support the usage of random-length filling for all cipher modes, and should also strongly consider requiring it for certain applications.

3) Confidentiality: Active attacks: It is important that SSL securely protect confidential data even against active attacks. Of course, the underlying encryption algorithm should be secure against adaptive chosen-plaintext/chosen-cipher text attacks, but this is not enough on its own. Recent research motivated by the IETF ipsec (IP security) working group has revealed that difficult active attacks on a record layer can break a system's confidentiality even when the underlying cipher is strong. One important active attack on ipsec is Bellovin's cut-and-paste attack [Bel96]. Recall that, to achieve confidentiality, link encryption is not enough, the receiving endpoint must also guard the sensitive data from unplanned confession. The cut-and-paste attack exploits the principle that most endpoint applications will treat inbound encrypted data differently depending on the context, protecting it more constantly when it appears in some forms than in others. The cut-and-paste attack also takes advantage of a basic property of the cipher-block chaining mode: it recovers from errors within one block, so transplanting a few consecutive ciphertext blocks between locations within a ciphertext stream results in a corresponding transfer of plaintext blocks, except for a one-block error at the beginning of the splice. In more detail, Bellovin's cut-and-paste attack cuts an encrypted ciphertext from some packet containing sensitive data, and splices it into the ciphertext of another packet which is carefully chosen so that the receiving endpoint will be likely to inadvertently leak its plaintext after decryption. The SSL record layer format is rather similar to the old vulnerable ipsec layout, so it is admittedly conceivable that a modified version of the attack might work against SSL. In any case, standard SSL-encrypting Web servers probably would not be threatened by a short-block type of attack, since they do not typically encrypt short blocks [3].

B. Message authentication

In addition to protecting the confidentiality of application data, SSL cryptographically authenticates sensitive communications. On the Internet, active attacks are getting easier to launch every day. We are aware of at least two commercially available software packages to implement active attacks such as IP spoofing and TCP session hijacking, and they even sport a user-friendly graphical interface. Moreover, the financial incentive for exploiting communications security vulnerabilities is growing rapidly. This calls for strong message authentication. SSL protects the integrity of application data by using a cryptographic MAC. The SSL designers have chosen to use HMAC, a simple, fast hash-based construction with some strong theoretical evidence for its security [4]. In an area where several initial ad-hoc proposals for MACs have been crypt analyzed, these provable security results are very attractive. HMAC is rapidly becoming the gold standard of message authentication, and it is an excellent choice for SSL. The SSL MAC keys contain at least 128 bits of entropy, even in export-weakened modes, which should provide excellent security for both export-weakened and domestic-grade implementations. Independent keys are used for each direction of each connection and for each new incarnation of a connection. The choice of HMAC should stop cryptanalytic attacks.

How SSL secure a transaction

Handshake

1. Client Hello: client side send hello message with a list of cipher suite which client supported, in this step client also create a random number: ClientHello.random.

2. Server Hello: server sends response of client hello message.Server will select a cipher suite, generate random number: ServerHello.random and session id.

3. Certificate Server sending certificate then client verifies it. Followed by server hello done.

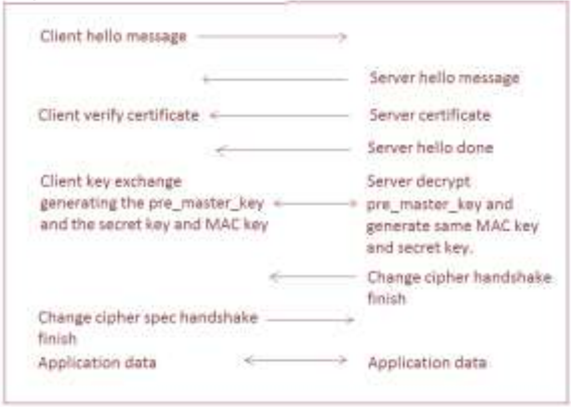
4. Client generates another random number: pre_master_secret (encrypted with server’s public key), then produce a master_key (structure in [5]).The master_key and two random number generated during the Hello procedure are used to create the secret key and MAC key.

5. Server decrypt the pre_master_key transmitted from client and generate a same master key as client.

6. Change cipher specification: send by client then client copies the pending cipher spec into the current cipher spec. at this point, client sends the finished message.

7. At same time, server is ready to transmit data encrypted with created secret key and also send a handshake finished message to client.

Figure:



Example of handshake using RSA public-key exchange

Problems with SSL

SSL is an excellent protocol. It is effective in the hands of someone who knows how to use it well, but is easy to use wrongly. There are many pitfalls that people fall into when deploying SSL, most of which can be avoid with a bit of work.

1. The merchant cannot constantly identify the cardholder. In cases where customers use stolen credit cards to initiate e-commerce transactions, merchants are responsible for card not present transaction charge backs. While SSL/TLS does provide the possibility of client authentication with the use of client certificates, such certificates are not mandatory and are hardly ever used. Still even if the client possesses a certificate, it is not automatically associated with his credit card. It means that, client might not be certified to use the credit card in question.

2. SSL only protects the communication link between the customer and the merchant. The merchant is allowed to see the payment information. SSL can neither guarantee that the merchant will not misuse this information.

3. Without a third-party server, SSL cannot provide promise of non-repudiation.

4. By chance SSL encrypts all communication data using the same key strength, which is unnecessary because not all data needs the same level of protection.

5. MITM attacks: MITM attacks fake a serious risk to many important SSL/TLS-based applications, such as Internet banking and remote Internet voting.

B. Secure Electronic Transaction (SET)

The Secure Electronic Transaction is an open encryption and security specification planned to care for credit card transactions on the Internet. The companies that collaborated in the development of SET include IBM, Microsoft, Netscape, RSA, Terisa and Verisign. It is supported by major corporations such as VISA Inc. and MasterCard. Although SET have been designed to operate in a wired infrastructure its transaction flow and implementation of security are of interest to us since it can also be employed in a wireless scenario.

The SET protocol is an advancement of the presented credit-card based payment system and provides improved security for information transfer as well as authentication of transaction participant identities by registration and certification. It is also an international standard. While SET permits customers to create credit-card payment to any merchant offering web-based services, customers also have the option of paying for other types of services using the on-line banking facilities.

In Secure Electronic Transaction (SET), merchant's website, secured web server and financial bank's server for the verification of customer's database makes an important role for successful transaction. Secure Electronic Transaction (SET) follows the following steps for successful electronic transaction:

1. The customer opens Master Card or Visa Card online payment system and fills all required information using his/her credit card.

2. The customer gets a copy of digital certificate generated by trusted certificate distribution authority. This certificate includes a public key and expiry time, which are required for secure online transaction.

3. Trusted third-party also receives certificates from the credit/debit card issuer bank.

These digital certificates include the public keys of bank and merchant.

4. The customer confirms the order through web page of merchant's website.

5. The web browser of customer validates the authenticity of merchant and confirms that the merchant is authentic and valid.

6. The web browser of customer transmits the order information to the merchant in encrypted format. This order information includes the public keys of merchant and bank and payment details.

7. The merchant authenticate the customer through verifying the digital signature on customer's certificate. This process may be occurred through bank as well as trusted third party.

8. The merchant transmits the order information to the concern bank. This information includes the

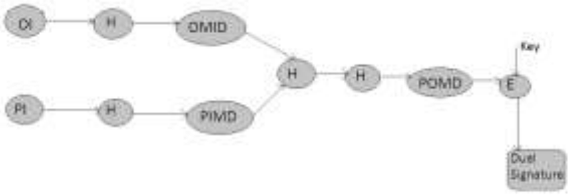
ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

bank's public key and customer's online payment information along with merchant's certificate.
9. The bank performs the several verification processes for the merchant and message authentication. Bank verifies the details of online payment, using digital signature on certificates.
10. The bank generates the final authorization for requested transaction to the merchant.
In such a way SET undergoes for various processes to perform electronic transaction in secure manner over wireless network.

DUAL SIGNATURE

- customer creates dual messages
  - order information (OI) for merchant
  - payment information (PI) for bank
- neither party needs details of other
- but must know they are linked
- use a dual signature for this
  - signed concatenated hashes of OI & PI

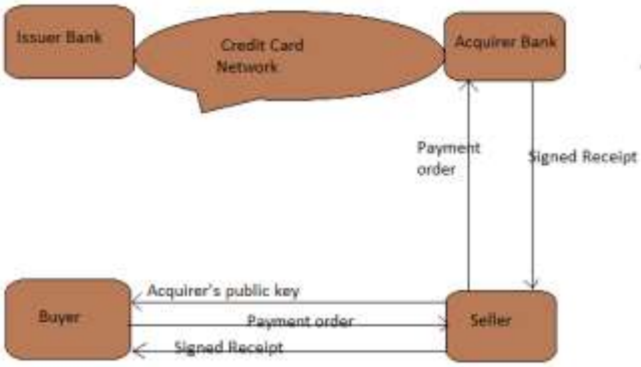
Figure:



Dual Signature

A Secure Electronic Transaction (SET) involves three parties: the credit/debit cardholder, the merchant, and a bank as a payment gateway. The credit/debit cardholder shares the order information with the merchant though merchant website but not with the bank (a payment gateway). But credit/debit cardholder shares the payment information with the payment gateway (bank) but not with the merchant. A set of dual digital signature establishes this partial sharing of information and allowing all communicating parties to confirm that they are performing the same transaction. In this process, each communicating party receives the hash format of the required information. The cardholder signs the hashes of payment and order information. Each communicating party can verify and confirm that the hash in their possession matches with the hash signed by the cardholder. The cardholder and merchant compute equivalent hashes for the bank to compare. All communications between communicating parties are highly protected. Merchants cannot access the credit card information of customer.
In SET, intruder or criminal is not able to make any transaction because it requires cardholder signature and a secret number received by trusted third party after registration. A merchant can be authorized to receive credit card numbers and has the option of accepting payments given a credit card number alone.

Figure:



Secure Electronic Transaction using Credit Cart

In Fig 3, whole process of Secure Electronic Transaction (SET) is shown. In this, SET involves three communicating parties as buyer, seller and the bank as a payment gateway. The online transaction is taking place over wireless network as Internet in secure manner.

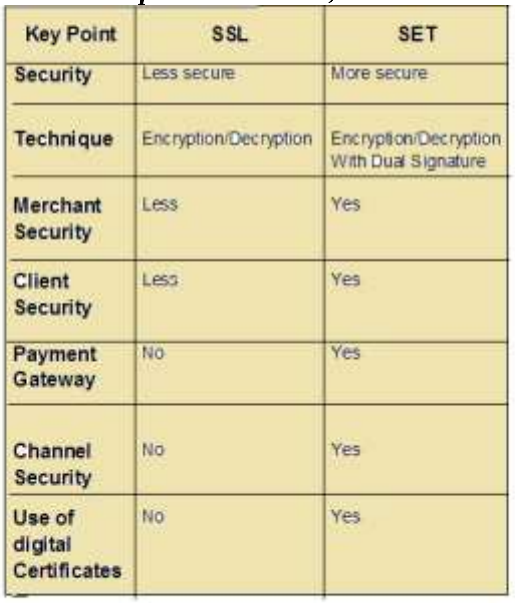
Authentication is an important issue for online users who perform online transactions over unreliable and insecure wireless network. All communicating parties must have faith in the authenticity of each other through trusted third party. In absence of authentication, any intruder or unauthorized user could pose as a merchant and tarnish the merchant's reputation by failing to deliver products and billing up the credit card bills in illegal manner. So, authentication is a critical factor to achieving trust in electronic commerce [6].
According to the Data Security for electronic transaction [7], the general steps for the SET are:
. Customer to Merchant
1) Customer sends both the order and payment details to the merchant, together with his certificate.

2) The payment details will be encrypted; merchant will not be able to read the payment details.
3) The merchant uses the customer certificate to verify the customer.
. Merchant to Customer's Bank
1. Merchant will send this payment details to his bank who will then forward it to the
customer's bank to request authorization that the customer has sufficient available
credit for the purchase.
Confirmation of Order
1. Once the authorization is received, the merchant will send an order confirmation to the customer.
. Shipping of Goods
1. Upon confirmation by the customer, the merchant will deliver the goods to the customer
. Request for Payment By Merchant
1. Lastly, the bank makes a request to the customer's credit card bank for payment.

Some disadvantages of SET are:

a) SET is designed for wired networks and does not meet all the challenges of wireless network.
b) As the SET protocol was designed to preserve the traditional flow of payment data (CA – MA –
Merchant's Bank), an end-to-end security mechanism was required.
c) The third element is the direction of the transaction flow. In SET transactions are carried out between Customer Agent and Merchant. It is vulnerable to attacks like transaction/balance modification by Merchant.
d) The transaction flow is from Customer to Merchant so all the details of the users credit cards/debit cards must flow via the merchant's side. It increases the user's risk, since data can be copied and used later to access a customer account without authorization.
e) There is no notification to the Customer from the customer's Bank after the successful transfer. The
user has to check his/her balance after logging on to his/her bank's website again.
f) SET is only for card (credit or debit) based transactions. Account based transactions are not included.
6. Comparison of Security Scheme for Secure Payment System

Table1: Compassion with SSL, SET.



Key Point	SSL	SET
Security	Less secure	More secure
Technique	Encryption/Decryption	Encryption/Decryption With Dual Signature
Merchant Security	Less	Yes
Client Security	Less	Yes
Payment Gateway	No	Yes
Channel Security	No	Yes
Use of digital Certificates	No	Yes

References

1. *http://www.webopedia.com/TERM/S/SSL.html*
2. *[Bel96] S. Bellovin, \Problem Areas for the IP Security Protocols", Proceedings of the Sixth USENIX Security Symposium, Usenix Association,1996, pp. 205-214 ftp://ftp.research.att.com/dist/ smb/badesp*.ps.
3. *[BCK96] M. Bellare, R. Canetti, and H. Krawczyk, \Keying Hash Functions for Message Authentication," Advances in Cryptology|CRYPTO '96 Proceedings, SpringerVerlag, 1996, pp. 1-15.*
4. *Brice Canvel. "Password interception in a SSL/TLS channel" Available at URL http://lasecwww.epfl.ch/memo_ssl.shtml*
5. *IBM Corporation. Cryptography and SET, June1998,Weblink:http://www.software.ibm com/comerce /payment/part2.html*
6. *Data Security for e-Transaction. Retrieved on April 12th 2008, from:http://www.comp.nus.edu.sg/~jervis /cs3235/set.html*