AN EVALUATED COMPARISON OF SSL AND SET

SANDEEP RAGHUWANSHI, PRANITA JAIN AND PATERIA R. K.
Department of Computer Science & Engineering, Maulana Azad National Institute of Technology (Deemed University), Bhopal, 462051, India, sandeep8056@yahoo.co.in , pranita.jain@gmail.com, r_k_pateriya@indiatimes.com

Abstract - Electronic payment lowers costs for businesses. The more payments they can process electronically, the less they spend on paper and postage. Offering electronic payment can also help businesses improve customer retention. The security of electronic payment protocols is of interest to researchers in academia and industry. While the ultimate objective is the safest and most secure protocol, convenience and usability should not be ignored, or the protocol may not be suitable for large-scale deployment. There are several e-payment methods proposed, but only a few are being used successfully. Electronic money systems are not as successful as credit-card methods. Credit card method has two poles as to fulfill its requirements SET (Secure Electronic Transaction) and SSL (Secure Socket Layer).SET payment-card based protocol. Although it is not specifically designed for electronic payment, Secure Socket Layer (SSL) based e-payment methods are at present the most widely used. The security of an e-payment method is very important for all parties involved in a transaction, but security alone does not guarantee success in the marketplace. An e-payment system must also be convenient. This requirement has different meanings for different parties. From the consumer’s point of view, “convenience” means to pay quickly and without an additional cost or too much effort. From the Financial point of view, “convenience” means low deployment and operational cost. The “convenience” requirement is generally ignored by security developers whose aim is to make the system as secure as possible. However, the aim should be to design a system which is both “secure” and “convenient”. In this paper we proposed an evaluated comparison of the two methods used in E payment based on their security and user convenience. The paper proposed the advantage and disadvantage of the methods from user all units involved in e payment point of view. A protocol can derived .which can take the advantages of the two methods. A protocol which is secure and convenient both.

Keywords: - SSL, SET, E-payment

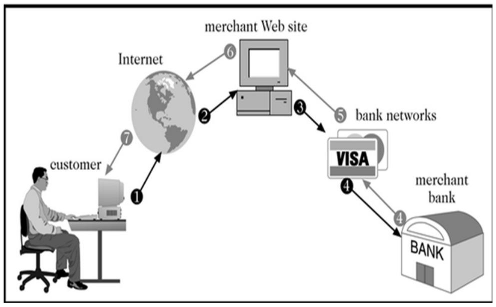
E-Payment

Electronic payment lowers costs for businesses. The more payments they can process electronically, the less they spend on paper and postage. Offering electronic payment can also help businesses improve customer retention. Basically e-payments system is used to transfer money over internet. Traditional methods are check credit or cash but e payment uses electronic cash, software wallets smart card or credit/debit cards. The basic requirements of e payment system are atomicity and non repudiation except these, money should be transferred electronically and universally accepted. E payment can be of following types.

E cash
Electronic wallets
Smart card
Credit card

In this paper we will explore the issues and solutions related to the credit cards e payment system.

The credit card system works as follows.



Payment Acceptance and Processing

Merchants must set up merchant accounts to accept payment cards. Law prohibits charging payment card until merchandise is shipped. Payment card transaction requires:

Merchant to authenticate payment card
Merchant must check with card issuer to ensure funds are available and to put hold on funds needed to make current charge
Settlement occurs in a few days when funds travel through banking system into merchant’s account

The security of electronic payment protocols is of interest to researchers in academia and industry. While the ultimate objective is the safest and most secure protocol, convenience and usability should not be ignored, or the protocol may not be suitable for large-scale deployment. There are several e-payment methods proposed, but only a few are being used successfully. Electronic money systems are not as successful as credit-card methods. Credit card method has two poles as to fulfill its requirements SET (Secure Electronic Transaction) and SSL (Secure Socket Layer).

SSL (Secure Socket Layer)

SSL is a protocol that provides a private, encrypted session between the client and the server. The protocol and its related certificates are widely used in web browsers. The server authenticates itself to the client using the server certificate, but the authentication of the client to the server is optional. In electronic payment terminology, server means merchant, client means consumer. In a basic electronic payment protocol based on SSL, a consumer sends account information and the transaction amount over an SSL protected connection. The merchant also sends the acknowledgment over the same channel. The authorization for the transfer of funds from the consumer's account is done as in classic Mail- Order/Telephone-Order transactions. This step is transparent to the consumer. Such a protocol is not only easy to implement but also minimally changes the traditional business model. Therefore it is very "convenient". The consumer does not need to register and obtain another account or card for electronic payment. The merchant and the FIs (Financial Institution) will make only slight modifications to the traditional authorization and settlement procedures. Some new interfaces may need to be implemented in order to provide automated responses to the consumer.

SSL Services-

Peer entity authentication

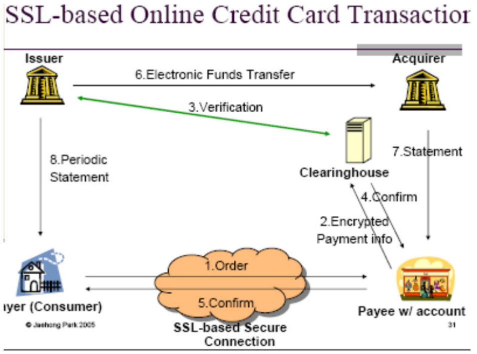
Data confidentiality

Data authentication and integrity

Compression/decompression

Generation/distribution of session keys integrated into protocol

Security parameter negotiation Cipher suite (key exchange method and cipher spec), compression algorithm



An SSL based protocol provides privacy, integrity and authentication of merchant to consumer. However, it does not guarantee the authentication of consumer to merchant and consumer non- repudiation. The consumer may deny making the payment and the merchant may not be able to prove the fact even if the transaction was legitimate.

SET (Secure Electronic Transaction)

Another class of electronic payment methods involves the FIs in the protocol. The most well-known method is the Visa and MasterCard joint effort, the *Secure Electronic Transaction* protocol. The interaction among FIs in the settlement network is not a part of SET. Communication between FIs and consumer/merchant is defined in the protocol. The authentication and non-repudiation requirements require the use of digital signatures and consequently of digital certificates for each message. Privacy and integrity are also attained. Each SET cardholder must have a digital certificate issued by a trusted Certificate Authority (CA). The cardholder's public key is certified via a digital certificate. This is necessary, because otherwise no one can be sure of the legitimacy of a cardholder's identity or of the public key. SET provides all necessary security requirements, unfortunately by sacrificing "convenience".

Followings are the points due to which SET have not attained a great attention from users.

1. SET requires the registration of consumers by their FIs. They need to have certificates in order to use the protocol.

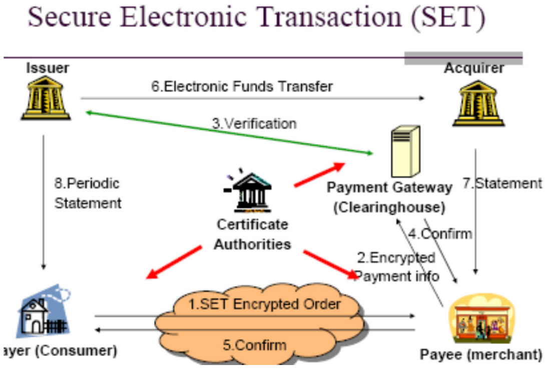
2. SET requires a PKI (Public Key Infrastructure). A PKI is a complete system for certificates. The FIs, the payment brands and the end users come together in a hierarchical manner in this PKI. The certificates are issued by independent CAs. We think that this PKI, as all other

distributed and large CA-based PKIs, is unlikely to be used, because the implementation and maintenance cost of this PKI, which is to be paid to CAs, would be an extra expense for the FIs.

3. SET is only for payment-card (credit or debit) based transactions. Account based transactions, like electronic check (e-check), are not included in SET.

Key Features of SET-

Confidentiality of cardholder account and payment information DES Integrity of payment information RSA digital signature, SHA-1 hash codes Cardholder account authentication X.509v3 digital certificates with RSA signatures Merchant authentication X.509v3 digital certificates with RSA signatures



An Evaluated Comparison:-

	SSL	SET
Authenticity	Fair Uses only the consumer's account information to establish identity.	Good Uses SET certificates and consumer's account information to check identity.
Privacy	Fair Uses Actual card number to make transaction at the risk of information being stolen.	Fair Uses Actual card number to make transaction at the risk of information being stolen.
Integrity	Uses Hash functions to ensure integrity.	Uses digital signature to ensures integrity.
Non repudiation	None	Uses digital signature to ensures integrity
Expansion	Good	Fair Process is complex.
Transaction cost	Same	A bit higher
Convenience	Good	Fair consumer's need to apply for SET certificates.
Acceptability	Good	Poor Need to construct entirely open PKI

Conclusion

In this paper we proposed an evaluated comparison of the two methods used in E payment based on their security and user convenience. The paper proposed the advantage and disadvantage of the methods from user all units involved in e payment point of view. A protocol may be derived which takes the advantage of the two discussed above.

References

[1] Raghuwanshi S., Pateria R.K., Singh R.P. (2009) *World Congress on Nature & Biologically Inspired Computing, 2009. NaBIC 2009*, 1665 - 1668.

[2] Levi A., Koç C. (2001) *17th Annual Computer Security Applications Conference (ACSAC'01)*, 0286.

[3] Electronic payment system- ISA 767 (2008) *Secure Electronic Commerce George Mason University*

[4] How SSL Works A brief Introduction to Secure Sockets Layer (SSL) Technology How SSL Works by Trustwave. htm http://www.verisign.com

[5] How Net Bill Works, Carnegie Mellon University (1997) www.netbill.com