Analysis of E-Commerce Security Protocols SSL and SET

Neetu Kawatra, Vijay Kumar
Dept. of Computer Science
Guru Nanak Khalsa College Karnal – India

ABSTRACT

Today is the era of information technology. E-commerce is the major achievement of this era. In E-commerce, the transaction takes place over the network. During various phases of an electronic transaction, the information such as product specification, order details, payment, and delivery information travels over the comparison of the two most popular E-commerce transactions secure protocols SSL and SET.

Keywords

Electronic Payment, SSL, SET, E-Commerce.

1. INTRODUCTION

Recent growth in Internet usage has increased the problem of privacy a lot. Every one using the web for E-commerce needs to be concern about the security of their personal information. But how it can be ensured is a big question and need to be solved. Following are the drawbacks of online payment systems regarding security:

- Unauthorized transactions or stealing money.
- Hacking of personal data and use it for identity theft.
- Attacking on data and make it corrupts.
- Take advantage of the convenience and speed of the electronic system to mask illegitimate or illegal transactions – i.e., money laundering.
- Take advantage of the efficiency of the electronic system to facilitate funding of illegal.

Thus Security is the major concern in E-commerce, which is the subject of this paper. Section II give the brief introduction of E-commerce, section III explain various electronic payment system, section IV discuss Security aspect of E-commerce , section V we will find a comparison study between two major E-commerce security protocols: SSL and SET, section VI about conclusion .

2. E-COMMERCE [1,5]

It is the ability to do business on-line via the Internet. With Internet based E-commerce, new types of transaction are appearing:

- Parties in the transaction such as business, consumers and government
- Things involved such as tangible and intangible good and services.

Also, it enhances the processes of the business and changes the way it delivers services to clients. In contrast, E-commerce comes also with some problems such as authentication and identification.

- Using a non-proprietary open network, Internet, with its associated security and reliability issues.
- Free client administration.
- On going Service availability.
- Geographically distributed parties.
- Parties' identity without physical contact.
- Support of off-line contact between parties through email, voice, fax, etc.
- The ability to collect data and parties profiles.

The typical E-commerce business application framework suppose to provide and support complete workflow function, where E-commerce has a massive workflow starts from account opening and end at payment protocol. Also, it should have a useful user interface foundation and service provision. Therefore, it is designed to consolidate main sub frameworks, and a service pool:

- Object Management Framework: this is responsible for sorting and retrieving all objects in the application. It also responsible for isolating the application from the underlying database.
- Business Logic Framework: the purpose of this to encapsulate the business rules and process independently of the user interface.
- User Interface Framework: the usage of this framework is to isolate the basic notion of a form from the underlying window system and operating system.
- Generic Service Pool: This can be called a virtual machine provides services to all other frameworks in a sufficiently abstracted form. So, the services can be implemented in several ways.

3. ELECTRONIC PAYMENTS METHODS [1]

There are several payment methods supporting electronic payments over the internet:

- Electronic payment cards (credit, debit, charge)
- Virtual credit cards
- E-wallets (or e-purses)
- Smart cards
- Electronic cash (several variations)
- Wireless payments
- Stored-value card payments
- Loyalty cards
- Person-to-person payment methods
- Payments made electronically at kiosks

4. SECURITY ASPECT OF E-COMMERCE SECURITY [4,6,7]

Security in E-commerce is very important part since communication can be easily intercepted, messages can be inserted, and the absolute identity of involved parties may be uncertain. There is a lack of a consistent and coherent set of protocols to cover the needs of merchants and consumers. However, one should minimize the effects of security failures on cyberspace for reliable electronic commerce systems.

Security tries to accomplish the following tasks:

- Authentication which identifies buyer and also makes sure that person is who he/she claims to be. Used methods are i.e. digital signature, finger prints, password or smartcards etc.
- Data integrity which means, that there must be a way to verify that data is not changed during the transactions.
- Confidentially must be preserved, so information concerning the tarns action are need to know basis.
- Non repudiation, which means that person who did the payments is not able afterwards deny doing so.

Among other considerations, it needs to consider the following important issues:

- ***Electronic Identification Strategy:*** It requires cryptographic security techniques to ensure transaction authentication and choose between secret key cryptography (SKC) MACing (Message Authentication Code) or public key cryptography (PKC) digital signatures.
- ***Level of Security****:* The determination of a security level will have impact on the type of electronic identification means given to clients. The choice is between logical securities in software-based authentication, or physical security if a security device is introduced into the picture.
- ***Client Authentication Strategy:*** With the PKC digital signatures, this issue is rooted in the PKI security model, and the role of certification authorities (CA). Where with SKC, the foremost options are the manual delivery of cryptographic keys or implied security model suggests the client enrolment.
- ***Confidentiality Requirements:*** Even if the critical aspect of E-commerce security is transaction authentication, confidentiality requirements are a significant design issue. This confidentiality requirements issue is independent from the selection of a security model. Obviously, when the confidentiality mechanisms are considered, the selection of SKC or PKC does matter.

5 E-COMMERCE SECURITY PROTOCOLS

5.1 Secure Sockets Layer (Ssl) [11,12]

In 1994, Netscape developed its first standard of Secure Socket Layer (SSL) to implement secure environment to exchange the information over the Internet and made it public for implementation in fall 1994. SSL is a security protocol protects communications between any SSL-enabled client and server software running on a network that uses TCP/IP, Gopher, FTP, Telnet etc.

SSL approach is to add a layer on top of the existing network transport protocol and beneath the application. This approach applied by adding an intermediate step, requiring negotiation of secure transmission options, to the establishment of a network connection. Data flowing between the client and the server on that connection is encrypted before transmission and decrypted before it can be used by the receiving system.

SSL Secured Connection Steps:

SSL steps to establish a secured connection between the customer client and server.

The figure shows the typical SSL connection establishment in order to transfer sensitive data over the internet (e.g. online shopping).

During SSL connection establishment only the server is authenticated using a digital certificate (authentication of the user usually occurs through user name and password after the SSL connection has been established).

SSL also offers the option for client authentication based on digital certificates.

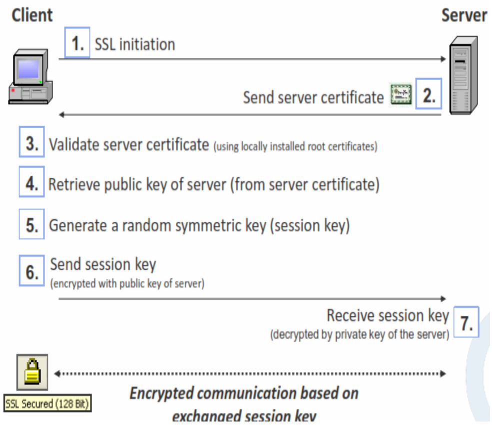
Client
Server
1. SSL initiation
Send server certificate
2.
3. Validate server certificate (using locally installed root certificates)
4. Retrieve public key of server (from server certificate)
5. Generate a random symmetric key (session key)
6. Send session key
(encrypted with public key of server)
Receive session key
(decrypted by private key of the server)
7.
SSL Secured (128 Bit)
Encrypted communication based on
exchanged session key

Fig 1: Ssl Secured Connection Steps

Advantages of SSL

- *Transparency* **-** since SSL provides security at the session layer, its presence is completely invisible either to the merchants' Web shop software or the customer. This is especially important for merchants because there's no cost for integrating SSL with their existing systems, other than the cost of installing the certificate.
- *Ease of use for customers* **-** SSL is already built into commonly used Web browsers and there is no need to install any additional software.
- *Low complexity* **-** the system is not complex, resulting in minimal impact on transaction speed.

Disadvantage of SSL

SSL has some serious problems when it comes to meet the security challenges of today financial sector.

- The merchant cannot reliably identify the cardholder. SSL does provide the possibility of client authentication with the use of client certificates; such certificates are not obligatory and are rarely used. Furthermore, even if the client possesses a certificate, it is not necessarily linked with his credit card.
- 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, nor can it protect it against intrusions whilst it is stored at the merchant's server.
- Without a third-party server, SSL cannot provide assurance of non-repudiation.
- SSL indiscriminately encrypts all communication data using the same key strength, which is unnecessary because not all data need the same level of protection. For example, a credit card number needs stronger encryption than an order item list. Using the same key strength for both creates unnecessary computational overhead.

5.2 Secure Electronic Transactions (Set)[9]

It is a standardized industry wide protocol specification designated to secure payment transactions and authenticate the parities involved in the transaction in any type of networks including Internet. VISA and MasterCard developed the SET standard with collaboration from leading software companies such as Microsoft, Netscape, RSA, VeriSign, and other.

SET was created to provide the trust needed for consumers. The protocol uses cryptography and digital certificates to provide confidentiality of the information, ensure payment integrity, and authenticate merchants, banks, and cardholders during SET transaction.

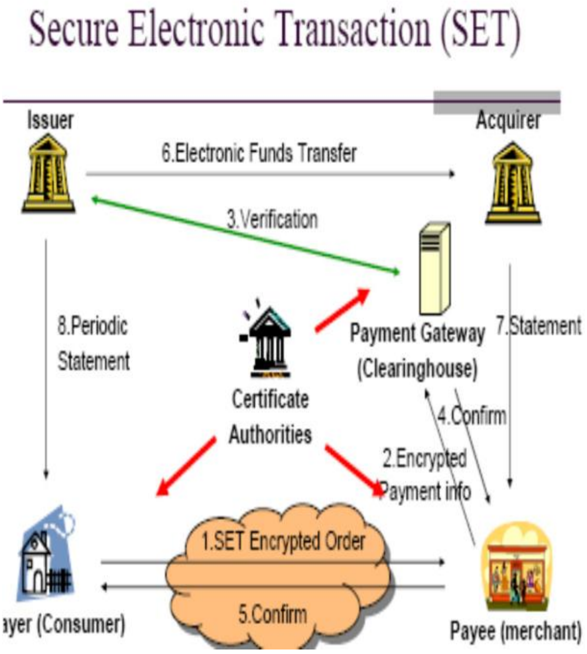

Fig 2: Secure Electronic Transactions

SET Specifications:

- SET uses RSA Data security public key cryptography in order to encrypt and decrypt transaction packets along with the use of digital certificates and digital signature for authentication of all parties to the transaction and validation that information has not been tampered with.
- SET makes online transactions even safer by using digital certificates to verify that consumers and merchants are both authorized to use and accept Visa cards. It's the electronic equivalent of a consumer looking for a Visa decal in a merchant's store window, and a merchant checking the consumer's signature on the back of a Visa card. Merchants worldwide are currently adopting SET.
- SET incorporates the use of public key cryptography to protect the privacy of personal and financial information. As a result, with SET, consumers' payment card information is protected all the way to the financial institution. The merchant cannot read this information in the payment transaction.
- With SET, cardholders can validate that the Internet merchant is legitimate through the merchant's digital certificate. SET software automatically checks that merchant has a valid certificate representing their relationship with their financial institution. This provides consumers with the confidence that their payments will be handled with the same Visa promise that they trust today.

Advantages of SET Protocol

- Confidentiality, authentication and data integrity was verified by a large collection of security proofs based on formal methods.

- In the standard variant of the protocol, SET prevents merchants from seeing the customer payment information, since this information is encrypted using the payment gateway's public key.
- To ensure merchant privacy, SET prevents the payment gateway from seeing the order information.

Disadvantages of SET

- The customer must install additional software, which can handle SET transactions.
- The customer must have a valid digital certificate.
- Implementing SET is more costly than SSL for merchants as well.
- Adapting their systems to work with SET is more complicated than adapting them to work with SSL
- Business banks must hire companies to manage their payment gateways, or install payment gateways by themselves.
- Despite being designed with security in mind, SET also has some security issues. In a variant of the SET protocol, the merchant is allowed to see the customer payment information, just as with SSL.
- SET employs complex cryptographic mechanisms that may have an impact on the transaction speed.
-

6. CONCLUSION

E-commerce is the ability to do business through the Internet. It is not just present of computers and absence of papers. It has more than this. E-commerce security is the major issue keeping many commerce organizations afraid from using Internet for their business. Secured Socket Layer (SSL) and Secured Electronic Transactions (SET) are the major popular E-commerce security protocols. Each one of them has its domain of use, its products, its strategy, and its own encryption procedure. Doing a comparison study between SSL and SET is not an easy thing. Using SSL or SET depends on user consideration. A comparison study shows the design issue of each one, its way of securing E-commerce, authenticates parties, using key exchange, and its encryption methodologies. While there are still lots of efforts focused on E-commerce security, it is not an easy decision to use Internet to exchange critical data such as credit card number, passwords, or any sensitive private information.

7. REFERENCES

[1] Singh Sumanjeet, " Emergence Of Payment Systems In The Age Of Electronic Commerce: The State Of Art", Global Journal Of International Business Research Vol. 2. No. 2. 2009

[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] Anup K. Ghosh. Certifying E-Commerce Software For Security. National Institute For Standards And Technology (NIST), 1999.

[5] Asuman Dogac, Electronic Commerce. Journal Of Database Management, Fall 1999.

[6] Marcus J. Ranum. Electronic Commerce And Security. V-One Corporation, White Paper. Http://Www.V-One.Com

[7] Shannon Matthews. Survey Reveals Ecommerce Security Systems Are Not Convincing Internet Users. World Research Inc. Aug. 20, 1999. Http://Www.Techmall.Com

[8] Anup K. Ghosh. Securing Electronic Commerce: Moving Beyond Cryptography. Journal Of Electronic Commerce, 1999.

[9] "SET Secure Electronic Transaction LLC. " Purchase, NY: SET Secure Electronic Transaction LLC, 2001. Available From Www.Setco.Org

[10] Marcus Goncalves. Industrial Networks Are Not Ready For E-Commerce. ARC Insights, Issue: 99-023, March 1999.

[11] Mayu Mishina. Is electronic commerce a good idea for you? AS/400 Systems Management, July 1998. Netscape Corp. Appendix E, Introduction to SSL. Page 213-229.

[12] Taher Elgamal. The Secure Sockets Layer Protocol (SSL). Danvers IETF Meeting, April 1995.

[13] Nikos Drakos. Security & Electronic Commerce:SSL Protocol. Security & Electronic Commerce Appendix, University of Leeds. 1997.

[14] Marvin A. Sirbu. Credits and debits on the Internet. IEEE-Spectrum, Feb. 1997.

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

An Evaluated Comparison