Review of online shopping security protocol of EC: SSL and SET

Vishakha Prabhakar Rode
Phd student
Department of management science
Dr.Bsbasaheb Ambedkar University ,Aurangabad

ABSTRACT:

At present 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 business, 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: *EC (Electronic commerce) SET (Secure Electronic transaction), SSL(Secure Socket Layer)*

1. Introduction

E-commerce can be mostly defined as a model of selling & buying process in which buyers are able to participate in all phase of a purchase judgment while stepping from beginning to end those processes by electronically rather than in a physical shop.

Nowadays the global network has become the main intermediator for conducting electronic commerce. Growth of the Indian ecommerce market is an outcome of increasing consumer accessibility to online e–commerce market is an outcome of rising consumer user-friendliness to the growing mobile internet penetration in the country. Desktop, notebook, & laptops are getting a go in favour of light weight access devices like tablets and smart phones, mobile internet is the new standard medium for access online.

In this paper we look the online shopping security of EC transaction take Review of the SET and SSL protocol.

2. Electronic payment system method

There are numerous payment methods supporting electronic payment and eCommerce over the internet.

*Electronic payment cards (Credit, Debit cards, virtual credit cards)

*E-wallets or (E-purse)

*smart cards

*Electronic cash

*Electronic value and payments

*loyalty cards

*person to person payment method

*payment made electrically at Kiosks

3. The important security aspects

The primary goal of cryptography is to secure vital data as it passes through a medium that may not be safe itself. Usually, that medium is a computer network. There are several different cryptographic algorithms, each of which can offer one or more of the following services to applications.
It is generally accepted that, in order to be considered secure, a payment system must assure the following fundamental security requirements.

3.1 Authentication

The assurance that the communicating parity is the one that is claims to be prevents the masquerade of one of the parties involved in the transaction. Both parties should be able to feel safe that they are communicating with the party with whom they think they are communicating. Applications generally perform authentication checks through security tokens or by verifying digital certificates issued by certificate authorities. Cryptography can help establish identity for authentication purposes.

3.2 Access Control.

The prevention of illegal use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.)

3.3 Data Confidentiality (Secrecy)

The protection of data from illegal disclosure. Confidentiality is an essential component in user privacy, as well as in the Protection of proprietary information, and as a deterrent to theft of information services. The only way to ensure confidentiality on a public network is through

strong encryption. Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium

3.4 Data Integrity (Anti-tampering)

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no medications, insertion, deletion, or replay). Prevents the unauthorized medication of data. Financial messages travel through multiple routers on the open network to reach their destinations. We must make sure that the information is not modified in transit.

3.5 Non-Repudiation

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of communication. • Non-repudiation, Origin- Proof that the message was sent by the specified party.
• Non-repudiation, Destination- Proof that the message was received by the specified party.
Non-repudiation is usually provided through digital signatures and public key certificates [2] [4] [10] [12].

4. Types of attacks on insecure system

4.1. Network Attacks
These easy services can be used to stop a wide variety of network attacks, including:
4.1.1. Snooping (passive eavesdropping)
An attacker watches network traffic as it passes and records interesting data, such as credit card information.

4.1.2. Tampering
An attacker monitors network traffic and maliciously changes data in transit (for example, an attacker may modify the contents of an email message).

4.1.3. Spoofing
An attacker forges network data, appearing to come from a different network address than he actually comes from. This sort of attack can be used to thwart systems that authenticate based on host information (e.g., an IP address).

4.1.4. Hijacking
Once a legitimate user authenticates, a spoofing attack can be used to "hijack" the connection.

4.1.5. Capture-replay
In some circumstances, an attacker can record and replay network transactions to ill effect.
For example, say that you sell a single share of stock while the price is high. If the network protocol is not properly designed and secured, an attacker could record that transaction, then replay it later when the stock price has dropped, and do so repeatedly until all your stock is gone.

4.1.6. PIN-guessing attack
An attacker can fake the digits and use the user authentication code (UAC) to launch a PIN-guessing attack.

4.2. Cryptographic attacks
In order to define the security level of a cryptosystem we have to specify the type of attack we are assuming (the power of the adversary) and the type of breaking which we wish to prevent (what tasks should the adversary be able to perform as the result of the attack) Given these specifications, we have to show that breaking the cryptosystem with the specified attack is as hard as performing a certain computational task. The types of attacks are.

4.2.1 Cipher text-only attack
Cipher text-only attack in which the adversary sees only cipher texts

4.2.2 known-plaintext attack
Known-plaintext attack in which the adversary knows the plaintexts (messages) and the corresponding cipher texts transmitted.

4.2.3 chosen-plaintext attack
Chosen-plaintext (CP) attack where the adversary gets to pick (adaptively) plaintexts of his choice and by exploiting the encryption mechanism he sees their encryption value.

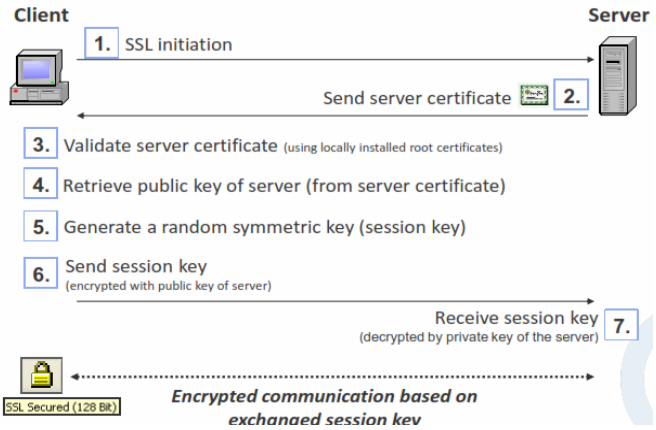
4.2.4 chosen-cipher text (CC) attack
Chosen-cipher text (CC) attack - where in addition to access to the encryption mechanism the adversary can pick (adaptively) cipher texts of his choice and by using the decryption mechanism (as a black box) he gets the corresponding plaintexts[5][8] [11].

5. E-COMMERCE Security Protocol

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



ig 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 itprotect 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 randomly 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

.

SET (Secure Electronic Transaction) vprotocol

Set protocol was developed by visa and MasterCard to provide security for credit card based payment transaction on the internet .SET address the following business requirements of confidentiality, integrity, authentication, and interoperability.

1) Confidentiality of payment information and order information that is transmitted along with the payment information.

2) Integrity of all data that is transmitted

3) Authentication that a cardholder is a legitimate user of a branded payment card account.

4) Authentication that a merchant can accept branded payment card transaction through his relationship with an acquiring financial institution.

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 make sure 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. Comparison of Security Scheme for Secure Payment System

Table1: Compassion with SSL, SET and Secure Tunnel

Key Point	SSL	SET Protocol.	Tunnel
Security	Less Secure	More Secure	More Secure
Technique	Encryption /Decryption	Encryption/Decryption-With Dual Signatures	Encryption /Decryption With-Crypto Tunnel
Merchant security	Less	Yes	More
Client Security	Less	Yes	More
Payment Gateway	No	Yes	More
Channel Security	No	Yes	Using Tunnel
Use of Digital Certificates	No	Yes	Yes

7. CONCLUSION Secure Electronic Payment schemes through SSL, SET, and secure communication tunnel have been reviewed in this paper. The security techniques are used to provide security the customer able to purchase the desired items. 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

8. 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.