Security in Electronic Payment Transaction

Fourcan Karim Mazumder, Israt Jahan, Utpal Kanti Das

Abstract— Security is the major concern in e-commerce. Internet is an insecure and unreliable media today. E-commerce applications are in danger to various security threats. The electronic payment system need 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 reduces the fraud that occurs with stolen credit card or debit card payment information and customer information. This paper illustrates that secure communication tunnel technique is a secure electronic payment system which can protect conventional transaction data such as account numbers, amount and other information.

Index Terms— Secure Socket Layer (SSL) protocol, Secure Electronic Transaction (SET) protocol, Authentication, Confidentiality, Integrity, Threat, Cryptography, Encryption, Decryption.

1 INTRODUCTION

INTERNET is broadly used for many purposes such as entertainment, communication; e-business etc. E-commerce is a significant part of e-business commonly known as electronic commerce. It refers to a wide variety of online business activities for products and services. Any type of business transaction in which the parties relate electronically rather than by physical exchanges or direct physical contact consists of the buying and selling of products or services over electronic systems such as internet and other computer networks comes under the type of e-commerce. Online transactions are an essential part of e-commerce. When we sell or buy an item we have to pay for it. Online payments are achieved with the help of online transactions (Srivastava et al., 2012). There is a widely perceived threat attached to payments made via the internet and this perception is in various circumstances justified. This is not like creation a phone call or sending a fax. The information sent from the customer to the web server may pass through several different stages before being delivered. The information is in digital form and at any phase an unauthorized individual may scan each message looking for credit card numbers (Nair, 2012). Customers may be at the risk for losing their private data since they may be unaware of the security aspect of performing on-line transactions (Hussain, 2013).

In order to perform the purchase, the participants require to exchange certain information over those links. If the information is transferred over the links in plain text, there is a possibility of eavesdropping. Anyone listening to the network traffic could achieve access to sensitive information such as card numbers, card type and whole detail of card holder. Credit card-such as a Master or Visa has a preset spending limit based on customer's credit limit. Debit Cards eliminates the amount of the charge form the cardholder's account and transfers it to the seller's bank. In electronic payment system, server stores records of each transaction. When the electronic payment system eventually goes online to communicate with the shops and the purchasers who can deposit their money and the server uploads these records for auditing reasons. Therefore, it is very essential to make the internet safe for buying and selling the goods on-line. Numbers of different security approaches are using to provide security in electronic transaction but these contains several problems (Singh et al., 2012). In this paper, it explains needs of security in electronic payment transaction, different kinds of threat in e-commerce, different types of security approaches in electronic transaction. Here it illustrates that secure communication tunnel is a secure payment system for electronic transaction. This secure electronic payment system uses different cryptographic algorithms and techniques to achieve privacy, integrity, authentication, non-repudiation etc.

- *Fourcan Karim Mazumder is currently working as Senior Lecturer in Computer Science and Engineering Department, International University of Business Agriculture and Technology (IUBAT), Dhaka, Bangladesh. E-mail: fk.mazumder@iubat.edu*
- *Israt Jahan is currently working as Associate Professor in Computer Science and Engineering Department, Jahangirnagar University, Savar, Dhaka, Bangladesh. E-mail:* isratju1@yahoo.com
- *Utpal Kanti Das is currently working as Associate Professor in Computer Science and Engineering Department, International University of Business Agriculture and Technology (IUBAT), Dhaka, Bangladesh. E-mail:* ukd@iubat.edu

2 Needs of Security in E-Commerce

In e-commerce, it is important to maintain proper security. Cryptography is a technique of mathematically encoding used to transform messages into an unreadable format in an effort to maintain confidentiality of data. Cryptography comprises a family of technologies that firstly include encryption transforms data into some unreadable form to guarantee privacy. Internet communication is like sending postcards where anyone who is interested can read a particular message; encryption presents the digital equivalent of a sealed envelope and then decryption is the opposite of encryption; it transforms encrypted data back into the original, clear format (Nair, 2012). The goal of cryptography is to secure essential data as it passes through a medium that may not be secure itself. There are many different cryptographic algorithms, each of which can offer one or more of the following services to applications. It is generally accepted that, a payment system must satisfy the following fundamental security requirements in order to consider security (Singh et al., 2012).

2.1 Authentication

Authentication is the method of verifying the identity of a process or device, often as a prerequisite to allowing access to resources in a system. The identity of a certain user or process is challenged by the system and appropriate steps must be taken to prove the claimed identity (Rane et al.,2012).The guarantee 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 experience comfortable that they are communicating with the party with whom they think they are communicating. Applications usually carry out authentication checks through security tokens or by verifying digital certificates issued by certificate authorities. Cryptography can help to launch identity for authentication purposes (Singh et al., 2012).

2.2 Access Control

The important network security concern addresses access control. In physical security, the term access control refers to restrict the entrance to a property, a building, or a room to authorized persons. Physical access control can be possible by a human, through mechanical means such as locks and keys, or through technological means such as a card access system. There are lots of technologies that can be used to control access to intranet and internet resources. Access control consists of authentication, authorization and audit. It also consist of measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers and monitoring by humans and automated systems. In any access control model, the entities that can carry out actions in the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects. Subjects and objects should both be deemed as software entities rather than as human users, any human client can only have an effect on the system via the software entities that they control. Although some systems equate subjects with user IDs, so that all methods started by a user by default have the same authority, this level of control is not fine-grained enough to satisfy the principle of least privilege (Farshchi et al., 2011).

2.3 Data Confidentiality

All data during the transactions has the request of being kept confidential. For example, account number and user name may be misused by others who have access to them; business prospect may be lost if order and payment information of your customer's are obtained by competitors. Thus, encryption is needed in the e-commerce data transmission (Ismaili et al., 2014).

2.4 Data Integrity

Integrity is one of the major concern of any business activity so as of e-commerce system. Integrity is categorized into two types such as integrity of transaction and delivery of product.

- Integrity of Transaction: When money is sent from consumer to supplier the integrity of operation must be maintained i.e. debit and credit of money must mapped in an integrated manner. Failure to do this will lead to a conflicting state which is highly undesirable.
- Delivery of Product: The customer must receive the goods in well condition before the payment for the product. It is impossible that the buyer pay the money without getting the product (Rattan et al., 2010).

2.5 Non-Repudiation

Non repudiation means that person who did the payments is not able afterwards reject doing so (Kawatra et al., 2011). This means not to refuse a sale or purchase implemented with digital signatures.

- Plaintext/Cleartext – text humans can understand.
- Ciphertext – text unreadable to peoples, uses encryption. Opposite process is call decryption.
- Cryptographic algorithm- It is called a cipher and it is a mathematical function. Most attacks are spotlighted on finding the key (Niranjanamurthy et al., 2013).

3 Types of Attack in E-Commerce Security

Several attacks or threats are available against e-commerce security such as

3.1 Snooping

Millions of computers are adding to the internet every month. Most users' awareness of security vulnerabilities of their systems is vague at best. Additionally, software and hardware retailers, in their quest to make sure that their products are easy to install, will ship products with security features disabled. In many cases, enabling security features needs a non-technical user to read manuals written for the technologist. The confused user does not effort to enable the security features. This makes a treasure trove for attackers (Aggarwal, 2014).

3.2 Tampering

An attacker monitors network traffic and maliciously modifies data in transit (for example, an attacker may alter the contents of an email message) (Singh et al., 2012).

3.3 Spoofing

Misrepresenting oneself by using false e-mail addresses or masquerading as someone else threatens integrity of site authenticity (Rane et al., 2012).

3.4 Hijacking

Once a valid user authenticates, a spoofing attack can be used to hijack the connection.

3.5 Capture-Replay

In some circumstances, an attacker can trace and replay network transactions to ill effect. For example, say that you sell a single share of stock while the price is much. If the network protocol is not accurately designed and secured, an attacker could record that transaction, then replay it afterward when the stock charge has dropped, and do so continually until all your stock is gone.

3.6 Pin-Guessing Attack

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

3.7 Cryptographic Attacks

In order to define the security level of a cryptosystem we have to indicate the type of attack we are assuming and the type of breaking which we hope to prevent. Given these specifications, we have to illustrate that breaking the cryptosystem with the specified attack is as tough as performing a certain computational task. Different types of attacks are:

- **Cipher Text Attack**
  Cipher Text-only attack in which the opponent sees only cipher texts.
- **Known-Plaintext Attack**
  Known-Plaintext attack in which the adversary familiars with the plaintexts and the corresponding cipher texts transmitted.
- **Chosen-Plaintext Attack**
  Chosen-Plaintext (CP) attack where the adversary gets to pick plaintexts of his selection and by exploiting the encryption method, he sees their encryption value.
- **Chosen-Cipher Text (CC) Attack**
  Chosen-Cipher Text (CC) attack - where in addition to access to the encryption method the adversary can pick cipher texts of his choice and by using the decryption method he gets the corresponding plaintexts (Singh et al., 2012).

4 Security Approaches to Secure Payment System

The successful operation of e-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure signature (Yasin et al., 2012). Different types of e-commerce security approaches are:

4.1 Digital Signatures and Certificates

Digital signatures provide the requisite for authentication and integrity. A sending message is run through a hash function and new value is produced known as message digest. The message digest and the plain text encrypted with the recipient's public key and send it to recipient. The recipient decrypts the message with its private key and transfers the message through the supplied hash algorithm. Digital certificate are also used for security functions. CA issues an encrypted digital certificate to applicant that holds the applicant's public key and some other identification information. The recipient of an encrypted message can use the CA public key to decode the digital certificate attached to the receiving message that's authenticate it as issued by the CA and then acquires the sender public key and identification information store within the certificate. Digital certificate includes the following information

- Certificate holder name
- Certificate expire data
- Certificate holder public key
- Signature of authority

An algorithm provides the ability to generate and validate signatures. Signature generation makes use of a private key to produce a digital signature (Yasin et al., 2012).

4.2 Secure Socket Layer (SSL) Protocol

The e-commerce business is all about making money and getting ways to make more and more money. But that's tough to if the consumers don't feel safe executing a transaction on your web site. Secure Socket Layer (SSL) is a commonly-used protocol for managing the security of a message transfer on the internet. When you have SSL, you are protected as well as your client (Hussain, 2013). Secure Socket Layer (SSL) is a protocol that encrypts data between the customer's computer and the site's server. When an SSL-protected page is requested, the browser recognizes the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing reverse and forth is encrypted so that a hacker sniffing the network cannot read the contents (Aggarwal, 2014).

SSL is an excellent protocol but is very easy to misuse. There are many drawbacks that people fall into when using SSL such as:

- The merchant cannot reliably recognize the cardholder. In cases where consumers use stolen credit cards to initiate e-commerce transactions, merchants are responsible for card not present transaction charge returns. While SSL does supply 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 essentially linked with his credit card. This means that the purchaser might not be authorized to use the credit card in question.
- SSL only defends the communication link between the customer and the merchant. The merchant is allowed to watch the payment information. SSL can neither assurance that the merchant will not misuse this information, nor can it protect it against intrusions whilst it is stored at the merchants' server.
- Without a third-party server, SSL cannot give guarantee of non-repudiation. So SSL protocol does not give facilities for non-repudiation.
- SSL indiscriminately encrypts all communication data using the same key strength, which is needless because not all data needs the same stage of protection.
- MITM attacks**:** MITM attacks create a serious threat to many relevant SSL-based applications, such as internet banking and remote internet voting (Singh et al., 2012).

4.3 Secure Electronic Transaction (SET) Protocol

It is a standardized industry wide protocol arrangement designated to secure payment transactions and authenticate the parties involved in the transaction in any type of networks including internet. VISA and MasterCard developed the SET standard with association from leading software companies such as Microsoft, Netscape, RSA, VeriSign and other (Kawatra et al., 2011). SET employs both symmetric and asymmetric cryptography to defend purchasing information sent between SET participants, including customer, merchant, the acquirer, and the issuer. Key management for SET is based on the use of a PKI to reliably allocate public keys between SET participants.

SET supports extended key lengths for both symmetric and asymmetric encryption. SET was designed to address the drawbacks in the security provisions for e-commerce that were not being fulfilled by SSL. SET presents an open standard not only for protecting the privacy but also for ensuring the authenticity of electronic transactions (Jarupunphol et al., 2013).

There are many disadvantages of SET protocol such as:

- Implementing SET is more costly than SSL for vendors as well. Adjusting their systems to work with SET is more complicated than adjusting them to work with SSL. Furthermore, vendors must have accounts opened at business banks competent of handling SET transactions.
- Business banks must hire companies to handle their payment gateways or install payment gateways by themselves.
- Despite being designed with security in mind, SET also has some security concerns. In a variant of the SET protocol, the merchant is allowed to watch the customer payment information. There are also some other, minor security matters in this protocol
- SET employs complex cryptographic methods that may have an impact on the transaction speed.
- Despite being very secure, SET has not been a success in e-commerce fields.
- The overheads related with SET are heavy. For a normal purchase transaction:
    a. Four messages are transferred between the merchant and customer
    b. Two messages are transferred between the merchant and payment gateway
    c. Digital signatures are calculated
    d. It is using 9 RSA encryption/decryption cycles
    e. It is using 4 DES encryption/decryption cycles and
    f. Four certificate authentications
- It has been argued by vendors that they have to expend lot of money in order to process SET transactions. From

buyer's point of view, they have to install proper software.

- Inter-operability trouble has not been solved.
- In SET protocol, the payment information is secure but order information is not secure (Singh et al., 2012).

4.4 3-D Secure

The main advantage over SSL is that 3-D Secures presents credit card authorization and non-repudiation. 3-D Secure is made upon the relationships between three domains named the acquirer, the issuer, and interoperability domains .The acquirer domain manages the relationship between the merchant and the acquirer. The issuer domain manages the relationship between the cardholder and the issuer. The interoperability domain holds the relationship between the acquirer and issuer domains. To protect the security of communication between the various entities, 3-D Secure needs the following links to be protected using SSL: cardholder merchant, cardholder-ACS, merchant Visa Directory, and Visa Directory-ACS.

Disadvantages of 3-D Secures such as:
The seller still has access to the payment information and all information is encrypted using the same key strength. The main benefit over SSL is that 3-D Secure provides credit card authorization and non-repudiation. On the other hand, prior customer registration is wanted (Singh et al., 2012).

4.5 Secure Electronic Payment System Using Secure Communication Tunnel

Secure electronic payment system consists of four system segments. The communication between the segments goes through secure communication tunnels. Secure communication tunnel means offer a secure way for communication between two or more parties or segments such as customer to merchant and merchant to payment gateway.

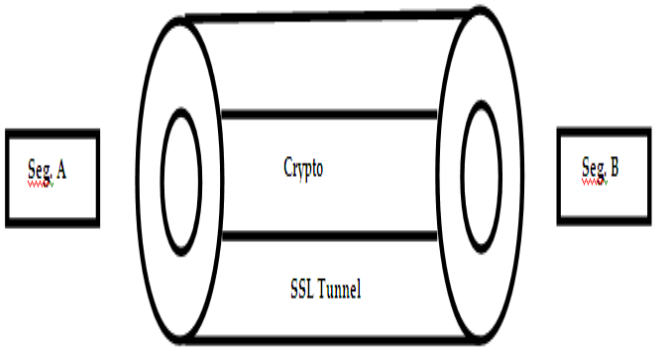

Figure: Secure communication tunnel consists of SSL and nested crypto tunnel.

Secure communication tunnel consists of SSL and nested crypto tunnel, which is formed by employing cryptographic algorithms and techniques on the information that are transmitted between parties. The SSL is stand on session key and crypto tunnel is stand on public key cryptosystem (Singh et al., 2012).

The purchaser decides to buy something and open the merchant's web site. Purchaser sees many item of merchant web site. At this time web server and web browser correspond through HTTP protocol. To be securing this system, secure communication tunnel and key cryptosystem is used to defend conventional transaction data such as account numbers, amount and other information.

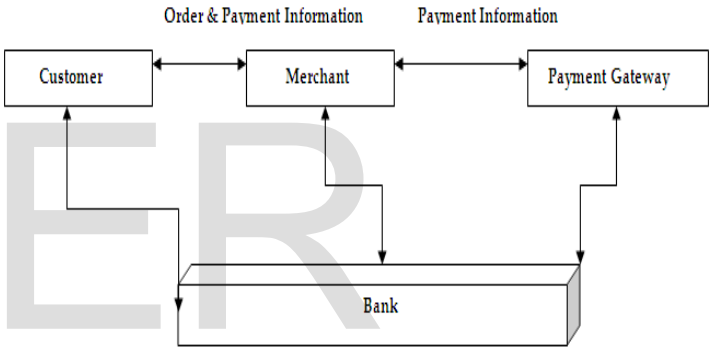

Figure: Secure communication tunnels between consumer, merchant and payment gateway.

Here web payment segment makes two messages.

- The first message holds order information.
- The second message holds payment information-credit card number and other information like credit card type and expiration date.

The order information is encrypted using symmetric session key and digitally signed using consumer's private key. The payment information is twice encrypted, first time using payment gateway public key and second time using symmetric session key. Retailer cannot peek the payment information because of the payment information is also digitally sign with the consumer's private key.

Comparisons among SSL protocol, SET protocol and secure communication tunnel are as follows (Singh et al., 2012):

Key Point	SSL	SET Proto-	Tunnel

		col	
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

Table: Compassion with SSL, SET and Secure Communication Tunnel

5 Conclusion

Information security has become a very vital aspect of modern communication system. Security objectives are achieved by cryptography functions and techniques. When customers and merchants carry out a transaction over internet, the protection of information against security threats is a key issue. Main benefits of security system for internet transaction are: it uses strong cryptography and authenticity checking models, the merchant is prevented from watching payment information, the customer can easy to use the system since he is not needed to install additional software for secure payments or to have a digital certificate. Here different approaches of security have presented that increases the level of security dimensions and shows that the security principle for secure communication channel has a significant level protection rather than unsecure communication channel.

References

[1] Srivastava, S., Bharti, R. (2012), 'Security Enhancement in Secure Electronic Transaction Protocol (SETP)', *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol. 2, No. 6, pp. 183-185.

[2] Nair, K. S. (2012), 'Providing Security and Safety in Electronic Commerce and Internet Transactions', *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, No. 2, pp. 462-465.

[3]Hussain , M. A. (2013), 'A Study of Information Security in E- Commerce Applications', *International Journal of Computer Engineering Science (IJCES)*, Vol. 3, No. 3, pp. 1-9.

[4] Singh, A., Singh, K., Shahazad (2012), 'A Review: Secure Payment System for Electronic Transaction', *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 3, pp. 236-243.

[5]Rane, P. B., Kulkarni, P., Patil, S., Meshram, B. B. (2012), 'Authentication and Authorization:Tool for Ecommerce Security', *Engineering Science and Technology: An International Journal (ESTIJ)*, Vol. 2, No. 1, pp. 150-157.

[6]Farshchi, S. M. R., Gharib, F., Ziyaee, R. (2011), 'Study of Security Issues on Traditional and New Generation of E-commerce Model', paper presented in the *International Conference on Software and Computer Applications IPCSIT vol.9, IACSIT Press, Singapore.*

[7]Ismaili, H. E., Houmani, H., Madroumi, H. (2014), 'A Secure Electronic Transaction Payment Protocol Design and Implementation', *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 5, No. 5, pp. 172-180.

[8]Rattan, M. V., Sinha, E. M., Bali, V., Rathore, R. S. (2010), 'E-Commerce Security using PKI approach', *International Journal on Computer Science and Engineering (IJCSE)*, Vol. 2, No. 5, pp. 1439-1444.

[9]Kawatra, N., Kumar, V. (2011), 'Analysis of E-Commerce Security Protocols SSL and SET', paper presented in the *National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) Proceedings.*

[10]Niranjanamurthy, M., Chahar, D. D. (2013), 'The study of E-Commerce Security Issues and Solutions', *International Journal of Ad-vanced Research in Computer and Communication Engineering*, Vol. 2, No. 7, pp. 2885-2895.

[11]Aggarwal, V. (2014), 'E-COMMERCE SECURITY ISSUES AND SOLUTIONS: A SURVEY', *GALAXY International Interdisciplinary Research Journal GIIRJ*, Vol. 2, No. 1, pp. 159-163.

[12]Rane, P. B., Meshram, B. B. (2012), 'Transaction Security for E-commerce Application', *International Journal of Electronics and Computer Science Engineering (IJECSE)*, Vol. 1, No. 3, pp. 1720-1726.

[13]Yasin, S., Haseeb, K., Qureshi, R. J. (2012), 'Cryptography Based E-Commerce Security: A Review', *IJCSI International Journal of Computer Science Issues*, Vol. 9, No. 2, pp. 132-137.

[14]Jarupunphol, P., Buathong, W. (2013), 'Secure Electronic Transactions (SET): A Case of Secure System Project Failures', *International Journal of Engineering and Technology*, Vol. 5, No. 2, pp. 278-282.