Cryptography Based E-Commerce Security: A Review

Shazia Yasin[1], Khalid Haseeb[2], Rashid Jalal Qureshi[3]

[1] Faculty of Physical and Numerical Sciences, Physics Department Islamia College (Chartered University) Peshawar, Pakistan

[2]Faculty of Physical and Numerical Sciences, Computer Science Department Islamia College (Chartered University) Peshawar, Pakistan

[3]Faculty of Physical and Numerical Sciences, Computer Science Department Islamia College (Chartered University) Peshawar, Pakistan

ABSTRACT

E-commerce is a powerful tool for business transformation that allows companies to enhance their supply-chain operation, reach new markets, and improve services for customers as well as for providers. Implementing the E-commerce applications that provide these benefits may be impossible without a coherent, consistent approach to E-commerce security. E-commerce has presented a new way of doing transactions all over the world using internet. Organizations have changed their way of doing business from a traditional approach to embrace E-commerce processes. As individuals and businesses increase information sharing, a concern regarding the exchange of money securely and conveniently over the internet increases. Security is a necessity in an E-commerce transaction. The purpose of this paper is to explain the importance of E-commerce security and will discuss pretty good privacy, secure E-commerce protocol, public key infrastructure, digital signature and certificate based cryptography techniques in E-commerce security.

Keywords *- Trusted Third Party, Pretty Good Privacy, Public Key Infrastructure, Certificate Authority, Digital Signature, Secure Socket layer, Secure Electronic Transaction, Secure E-commerce Protocol.*

1. INTRODUCTION

Security must be part of the design. If we do not design our application with security in mind, we are doomed to be constantly addressing new security vulnerabilities. Careful programming cannot make up for a poor design [1].E-commerce refers to a wide range of online business activities for products and services. Security is the basic need to secure information on internet [2].E-commerce transaction between customer and merchant can include different requests. The high degree of confidence is needed in authenticity and privacy of such transactions can be difficult to maintain where they are exchanged over an untrusted public network such as the Internet [3]. It also pertains to any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact. A security objective is the contribution to security that a system is intended to achieve.E-commerce is conducted on global network that is Internet which is untrusted. Therefore confidentiality is required during transaction and sending information should be kept secure against all type of threats. Security has emerged as an increasingly important issue in the development and success of an E-commerce organization. Gaining access to sensitive information and replay are some common threats that hackers impose to E-commerce systems [4].

2. SECURITY IN E-COMMERCE

The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure [5]. Each phase of E-commerce transaction has a security measures.

Table 1: Security measures in different phases of E-commerce Transaction

E-commerce Transaction Phases			
Information Phase	Negotiation Phase	Payment Phase	Delivery Phase
Security Measures			
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encry-ption	Secure Delivery Integrity Checks

A general model has been introduced by Schmid who identifies three phases for most processes in E-commerce:

i. During the information phase the parties try to find partners, compare them, clarify their trade relation, and specify the products to be exchanged. These actions are not legally binding.
ii. In the contracting phase the parties decide on their partners according to their decision criteria and work out and sign a contract about their trade relation.
iii. Finally, in the delivery phase payment and delivery is done and eventually a new transaction is prepared [6].

The key dimensions of E-commerce security are:

i. Access Control.
ii. Privacy/Confidentiality.
iii. Authentication.
iv. Non Repudiation.
v. Integrity.
vi. Availability.

2.1 Security in E-commerce

In E-commerce security the trust models are classified into three main categories [7].

2.1.1 Hierarchical

In this trust model, the hierarchy consists of a series of CA authorities that are arranged based on a predetermined set of rules and conventions. However, a failure of a single CA will corrupt the entire trust model and potentially all certificates signed by it.

2.1.2 Distributed

In this trust model no CA is involved. There is no trust party involved during transaction. PGP uses this type of trust model for email security. This trust model does not perform well into the internet based E-commerce because each party left to its own device to determine the level of trust that it will accept from other parties.

2.1.3 Direct

This trust is also known as peer to peer trust model. It is used in symmetric key based systems. In this trust model no trusted third party is involved. Direct trust model is not well for internet based E-commerce.

3. RELATED WORK

Several research papers have been presented discussing security aspects in E-commerce.

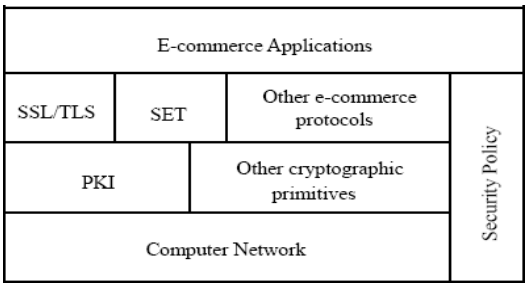

Fig. 1 General model of E-commerce Security[8]

E-commerce software packages should also work with Secure Electronic Transfer , Secure Socket Layer, Public Key Infrastructure and Secure E-commerce protocol [3] technologies for encryption of data transmissions.E-commerce operates on Internet or intranet. The main E-commerce transaction models are B2B and B2C. In order to identify or authenticate the identity of the other party on the Internet, public key infrastructure (PKI) offers the best way for this requirement. Based on PKI several security services can be implemented to secure E-commerce transaction. The below notation depicts the concept of PKI encryption technique. In this system, suppose that the receiver, Bob, has private key and public key are (PR_R) and (PU_R) respectively. Receiver's public key (PU_R) is publicly known and used for encryption and receiver's private key (PR_R) is kept secret, used for decryption. Suppose that the sender, Alice, wants to send an original secret message (SM) to the receiver (Bob), Alice (the sender) will encrypt her secret message (SM) using Bob's public key (PU_R) to get the encrypted secret message, that is known as cipher message (C), and sends it to Bob (the receiver). The receiver (Bob) can decrypt the cipher message (C) by using only his private key (PR_R).

$$C= E (PU_R(SM))$$
$$SM=D (PR_R(C))$$

3.1 Digital Signatures and Certificates

Digital signatures provide the requirement for authentication and integrity. A sending message is run through a hash function and new value is generated known as message digest. The message digest and the plain text encrypted with the recipient's public key and send to recipient. The recipient decrypts the message with its private key and passes the message through the supplied hash algorithm. Digital certificate are also used for security purposes. CA issues an encrypted digital certificate to applicant that contains 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 verify it as issued by the CA and then obtains the sender public

key and identification information store within the certificate. Digital certificate contains the following information

i. Certificate holder name
ii. Certificate Expire data
iii. Certificate holder public key
iv. Signature of authority

An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature [10].

3.2 Secure Socket Layer

Secure Socket Layer (SSL) was developed by Netscape to provide secure communication between web servers and clients. The information is broken into packets, numbered sequentially, and an error control attached. Individual packets are sent by different routes [11]. SSL is widely used on the Internet, especially for interactions that involve exchanging confidential information such as credit card numbers [12]. SSL uses PKI and digital certificates to ensure privacy and authentication [11]. SSL protects the communication between a client and a server and provides authentication to both parties to secure communication [13]. SSL encryption is at transport layer rather then Application layer. SSL provides point to point security [14] .Message is encrypted only during transmission over the network and other security mechanisms are required to handle security of the messages in an Application or disk. SSL is above TCP layer and below application layer. SSL allows many key exchange algorithms, but some algorithms such as Diffie-Hellman key exchange have no certificate concept [8]. It is used to exchange secret key securely between communication parties.

3.3 E-commerce Based on Pretty Good Privacy

PGP is the result of Phil Zimermann efforts. It provides a secure communication in an unsecured Electronic environment.PGP provides authentication and confidentiality, compression and segmentation services for Email Security.PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications [15]. It is widely used for email security.

3.3.1 Authentication

On sender side SHA-1 is used to generate a 160-bits hash code of the sending message. The hash code is encrypted using the sender's private key and the result is appended to the message. The receiver decrypts the hash code by sender public key. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If both hash codes are same then the message is authentic.

3.3.2 Confidentiality

The sender creates a message that is to be transmitted and a 128-bit number to be used as a session secret key for the sending message. The message is encrypted using 3DES with the session secret key. The session secret key is again encrypted using the recipient public key and is appended to the sending message. The receiver used its private key to decrypt and recover the session secret key and then session secret key is used to decrypt the sending message.

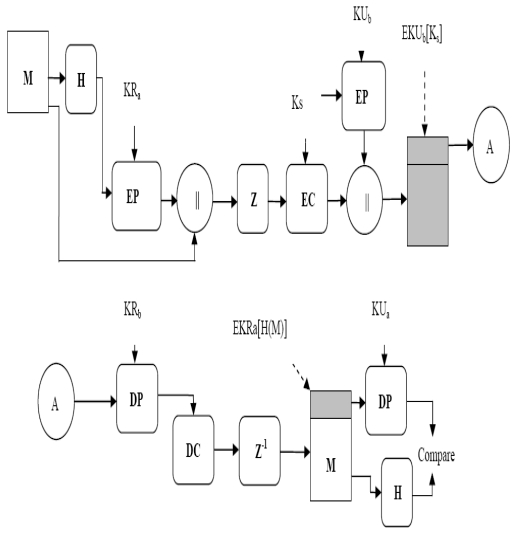

Fig.2 PGP Cryptographic Functions[15]

Fig. 2 depicts the following steps that are performed by PGP to sender side

i. Hash of Message H(M) is calculated.
ii. Hash is encrypted using private key of user A (KR_a) and it is concatenated with message M.
iii. Then Compression (Z) is done using winzip
iv. After compression PGP perform symmetric encryption using sesion key(Ks) and session key also encrypted using public key of user B (KU_b)
v. At the end PGP perform concatenation and transmitted to user A

Fig. 2 shown the following steps that are performed by PGP to receiver side

i. Decrypt the session key using private key of B (KR_b)
ii. Then using the decrypted session key recover the message.
iii. Uncompress the message (Z^{-1}) and decrypt the message hash using public key of user A(KU_a)
iv. Calculate the hash of message and compare with sender's calculated hash value .
v. If both hash are same then message is authentic

Table 2: PGP Cryptography Notations

Notation	Description
M	Message
H	Message Hash
EP, DP	Public Key Encryption & Decryption
EC, DC	Symmetric Encryption &Decryption
Ks	Session Key
KR_a , KR_b	Private key of user a and b
KU_a, KU_b	Public Key of user a
Z , Z^{-1}	Compression &Uncompression
||	Concatenation

3.3.3 Public Key Infrastructure

PKI provides a foundation for other security services. The purpose of a PKI is to allow the distribution and use of public keys and digital certificate to provide secure communication. There are some popular public-key encryption algorithms, for example, RSA, ElGamal, and ECC. The security of the most public-key encryption algorithms is based on discrete logarithms in finite groups or integer factorization [1][16][17]. A PKI is a foundation on which other applications and network security components can build. Systems that often require PKI based security mechanisms include E-mail, various chip card applications, value exchange with E-commerce, home banking, and electronic postal systems.

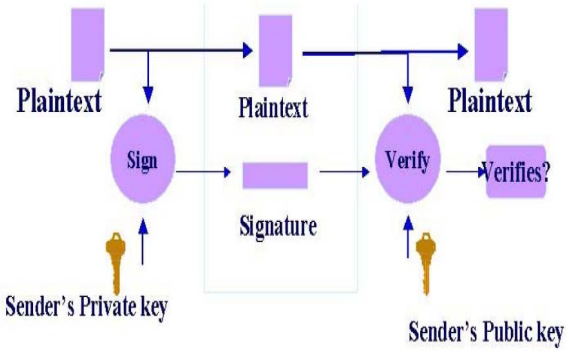

Fig. 3 Public Key Infrastructure

In above figure sender encrypts plain text with his/her private key and concatenate plaintext with signature. When receiver receives then receiver decrypt it using sender public key. This shows the authentication using PKI.
The discovery of public key cryptography has made a number of services available, some of which were either unknown or unachievable with symmetric ciphers [18]. One of the main branches and applications of the public-key cryptography is a public-key encryption scheme which allows two parties to communicate securely over an insecure channel without having prior knowledge of each other to establish a shared secret key[19].The process employs certificates which are issued to users or applications by a certificate authority (CA). Issuance of a certificate requires verification of the user's identity usually by a registration authority (RA). PKI uses digital certificates to protect information assets through the following mechanisms:

i. Authentication: Validates the identity of machines and users.
ii. Encryption: Encodes data to guarantee that information cannot be viewed by unauthorized users or machines.
iii. Digital signing: Provides the electronic equivalent of a handwritten signature and also enables enterprises to verify the integrity of data and determine whether it has been tampered with in transit.
iv. Access control: Determines which information a user or application can access and which operations it can perform once it gains access to another application also called authorization.

3.3.4 Secure E-commerce Protocol

A Secure E-commerce Protocol provides a certificate based security machanism. In this scheme both customer and merchant request CIA for issue certificates so both can initiate their transaction. Both parties will authenticate each other by their ID's. In this approach nonce is used to handle replay threat. Customer and Merchant certificates schema are shown in fig 4,5. The schema contains ID, certificate serial number, issuer name, purpose of certificate ,certficate hash code , start date , expire date etc. Certificate is encrypted by private key of CIA ($EPR_{(CIA)}$).

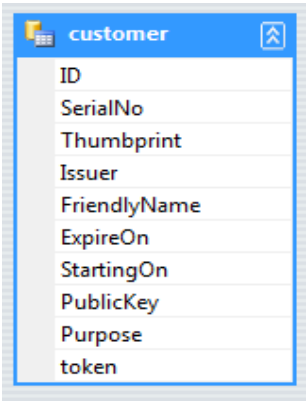

Fig 4: Customer Certificate Schema

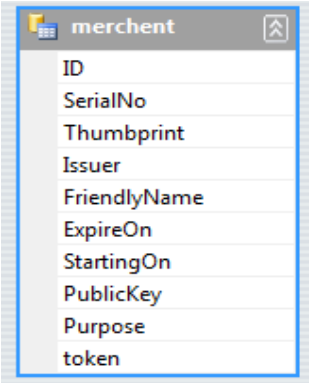

Fig 5: Merchant Certificate Schema

Table 3: SEP Steps

i.	$E_{KU\ (Auth)}$ [ID_A, Req_A, Time, K_{UA}, N_A]
ii.	$E_{KU\ (Auth)}$ [ID_B, Time, K_{UB}, N_A]
iii.	C_A=$E_{KR\ (Auth)}$ [ID_A, Req_A ,Time, K_{UA}, N_A]
iv.	C_B=$E_{KR\ (Auth)}$ [ID_B, Time, K_{UB}, N_B]
v.	$T_A \rightarrow M$
vi.	$T_B \rightarrow C$
vii.	$E_{ku\ (B)}$ [N_1, $E_{KR\ (A)}$ [ID_A, Time, N_A]]
viii.	$E_{ku\ (A)}$ [N_2, $E_{KR\ (B)}$ [ID_B, Time, N_B]]
ix.	$E_{ku\ (B)}$ [$E_{KR\ (A)}$ [N_2]]

Secure E-commerce Protocol[3] provides security against Authentication , Confidentiality , Integrity, Non Repudiation ,Replay attack and man in the middle attack.

Table 4: SEP Notations

Notation	Description
CIA	Certificate Issue Authority
C_A, C_B	Certificate issue to user A
$N_{1,\ N2}$	Nonce generated by user A
Time	Time Stamp
ID_A, ID_B	Identity of user A and B
$E_{KR(A)}$, $E_{KR(B)}$, $E_{KU(A)}$, $E_{KU(B)}$	Encryption using private/public keys of user A and B

4. FUTURE WORK

Information security is a burning issue in research community. Pretty good privacy can be used to provide authentication and confidentiality to E-commerce security but it is not a fool proof solution because integrity, Non repudiation and replay threats are also important E-commerce security dimensions. Secure E-commerce protocol provides protection to a single transaction at a time it cannot handle multiple E-commerce transactions at a time.

5. CONCLUSION

Information security has become a very critical aspect of modern communication system. Privacy, integrity, confidentiality and non repudiation are main security dimension to protect E-commerce transactions against threats. These objectives are achieved by Cryptography functions and techniques. When customers and merchants perform a transaction over Internet, the protection of information against security threats is a major issue. During sending the sensitive information, the data must be protected from unauthorized access to maintain its privacy and integrity. In this research paper different approaches has presented that increases the level of security dimensions using cryptographic techniques.

6. REFERENCES

[1] Thomas L. Mesenbourg, "An Introduction to E-commerce", Philippines: DAI-AGILE, 2000
[2] William Stallings, "Cryptography and Network Security", 3rd edition, Prentice
[3] Khalid Haseeb, Dr. Muhammad Arshad, Shoukat ali and Dr. Shazia Yasin " Secure E-commerce Protocol", International Journal of Computer Science and Security (IJCSS), Vol. 5 No. 1, pp.742-751, April 2011
[4]D. Berlin, "Information SecurityPerspective on Intranet," presented at Internet and E-Commerce Infrastructure, 2007.
[5] S. R. S. KESH, AND S. NERUR, "A Framework for Analyzing E-Commerce Security," Information Management and Computer Security, vol. 10, no. 4, no. pp. 149-158.
[6] Schmid.B,"Elecktronische Markte". p 465-480. 1993
[7] Joel Weise, "Public Key Infrastructure", SunPSSM Global Security Practice Sun BluePrints™ OnLine August 2001
[8] QIN Zhiguang, LUO Xucheng, GAO Rong, " A survey of E-commerce Security", School of Management, University of Electronic Science and Technology of China Chengdu, Journal of Electronic Science and Technology of China Vol.2 No.3, Sept 2004
[9] Abdullah M. Jaafar and Azman Samsudin, A New Public-Key Encryption Scheme Based on Non-Expansion
[10]P. C. O. A.J Menezes, and S.A. Vanstone, Handbook of Applied Cryptography: CRC Press, 1996.
[11] An Introduction to Cryptography (found in the documentation of PGP® Desktop 8.1). Page 17. June 2004.
[12] Jagdev Singh Kaleka, "E-Commerce: Authentication & Security on Internet", Deptt. of Technical Education and Industrial Training, Govt. of Punjab
[13] Cetin K. Koc, "Next Generation E-Commerce Security" Information Security Laboratory December 2, 1999

[14] Aiman H. Mufti, Saudi Armco, "e-Commerce and its Security", February 11, 2001
[15] Nada M. A. Al-Slamy, "E-Commerce Security", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008
[16] J. J. Amador, and R. W. Green, "Symmetric-Key Block Cipher for Image and Text Cryptography", International Journal of Imaging and Technology, Vol. 15, No. 3, (2005), pp. 178-188.
[17] C.-S. Laih, and K. Y. Chen, "Generating visible RSA public keys for PKI", International Journal of Information Security, Vol. 2, No. 2, Springer-Verlag, Berlin, (2004), pp. 103-109
[18]Dale Barr, "Public Key Infrastructure", TECHNOLOGY AND PROGRAMS DIVISION Volume 11, Number 3, December 2004 Visual Cryptography and Boolean Operation, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 2, July 2010.

[19] Abdullah M. Jaafar and Azman Samsudin," A New Public-Key Encryption Scheme Based on Non-Expansion Visual Cryptography and Boolean Operation", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 2, July 2010

Shazia Yasin did her phd from university of Cambridge, U.K. She has 28 research international publications and 8 national publications. Her impact factor is 49.She did Post-Doc from University of Cambridge. Her field of interest is nanotechnology, transport in liquid and cryptography. Currently she is the Associate Professor and Chairperson of Physics Department, Islamia College Peshawar (Chartered University).

Khalid Haseeb is a Lecturer in Computer Science Department, Islamia College Peshawar (Chartered University). He did M.Sc in Computer Science from University of Peshawar, Pakistan. He did his MS-IT from im|sciences Peshawar, Pakistan. He did 7 research papers in international conferences and journals. He obtained international network certifications from Microsoft and Cisco. His research area is cryptography and network security.

Rashid Jalal Qureshi is a Assistant Professor in Computer Science Department, Islamia College Peshawar (Chartered University). He did phd in Computer Science from Université François-Rabelais de Tours, Tours, France.He did Post-Doc from University of Debrecen, Debrecen, Hungary.He did several research papers in international conferences and journals. His research area is computer graphics, image processing and visual cryptography.