International Journal of Computer Science
Oddity...Probe...Reviste...

http://www.ijcsjournal.com Volume 3, Issue 1, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-072 PAGE NO: 413-416.

Cryptography security in Online Transaction- A Current Scenario

Zeenat Hasan[#1], Dr. C.P.Agrawal[*2]

[#]*Research Scholar Computer Science & Application Department*
MCNUJC, Bhopal ,India

[*]Professor Computer Science & Application Department
MCNUJC, Bhopal, India

[1]zeena_hasan@rediffmail.com
[2]agrawalcp@yahoo.com

***Abstract*— Online transaction is a powerful tool for business expedition that allows different companies to increase their sale through reaching new market and improve customer service. Here people are not interacting directly but rather then they are interacting through electronically therefore business requires coherent ,consistent environment for online transaction. The objective of this paper is to explain the importance of online transaction security and different aspects of it. This research paper presented different ways have presented that increases security level using cryptographic techniques.**

.

***Index Terms*— Third Party, Public Key Infrastructure, Certificate Authority, Digital Signature, Secure Socket layer**

I. Introduction

Online transaction changed the way people were doing business ,now a days people buy and sell things and provide goods and services directly from PC,Mobile. There fore Online transactions require secure environment so that people and business should no worry about outsiders stealing their identity and data to gain access to their valuable information just like credit cards or banking information[1]. If online transaction wants to be part of a business for a long time then it must provide security and trust and that is the place where cryptography security come in to the picture.[2]

II. Security in Online Transactions

For successful online transaction there must be coordination among several applications development platforms, database management systems, systems software and network infrastructure, and in each phase security is required[4].

The key dimensions of E-commerce security are:

- Access Control.
- Privacy/Confidentiality.
- Authentication.
- Non Repudiation.
- Integrity.
- Availability.

A. *Online Transaction Phases and Security in Each Phase*

1) *Information Phase:* In this phase information is provided to the customer who wanted to purchase the product .In this phase following security measures are taken into account;

- Confidentiality
- Access Control
- Integrity
- Checks

2)Negotiation Phase: In this phase negotiation is done between customers and sellers. They might offer different offers and schemes to the customers. In this phase following security measures are taken into account;

- Secure Contract
- Identification
- Digital Signature

*3)Payment Phase***:**In this phase Payment options are given by sellers to customers. This options may be net banking through credit card ,debit card etc. Therefore in this phase we require strict encryptions techniques.

4)*Delivery Phase*:In this phase product must be delivered on that place which is given by customers. In this phase following security measures are taken into account;

- Secure Delivery
- Integrity Checks

.

B. Security in E-commerce

In E-commerce security the trust models are classified into three main categories [5].

*1)Hierarchical***:**In this trust model there must be hierarchy among different authorities involved
in online transaction but drawback is that failure of a single authority corrupt whole trust model.

2)*Distributed***:**In this trust model no Certified Authority is involved. There is no trust party involved during transaction. This type of trust model for email security. This trust model does not perform well in online transactions because each party left to its own device to determine the level of trust that it will accept from other parties.

c)*Direct***:**Another name of this model is peer to peer trust model. It is used in symmetric key based systems. In this rust model no trusted third party is involved. Direct trust model is not well for internet based E-commerce.

III. Different Cryptography formats used in Online Transactions

*1)Secure Socket Layer***:**Secure Socket Layer (SSL) was developed by Netscape for providing secure communication between seller and buyer. The information is broken into packets, numbered sequentially, and an error control attached. Individual packets are sent by different routes [6].In transaction confidential information such as credit card number ,debit card number are exchanged through SSL[7] .SSL layer provides authentication at both the ends seller as well as buyer. SSL encryption is at transport layer rather then Application layer and provide point to point security[8]. Through this layer message is encrypted only during transmission over the network.This layer also supports exchange of secret key securely between buyer and seller.

2)*Digital Signature*: When big deal of transaction is done then along with a document digital signature is also sent for authentication and integrity .

*3)Secure E-commerce Protocol***:** It adopts certificate based security mechanism. In this process both customer and seller request third party for issuing certificate that is used for initiation of their transaction.Both customer and seller will authenticate each other by their ID's.

4) Public Key Infrastructure: PKI provides base for other security services such as

a. Authentication: Validates the identity of machines and users[9].

b. Encryption: Encodes data to guarantee that information cannot be viewed by unauthorized users or machines.

c 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.

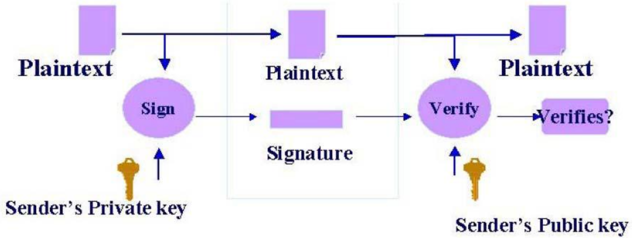

Fig. 1 Public Key Infrastructure [10]

IV. CONCLUSION

Security has become a very critical aspect of modern online transaction . Integrity, privacy, confidentiality and non repudiation are main security dimension to protect online transactions against threats. These objectives are achieved by Cryptography functions and techniques. when people perform a transaction over internet then protection of information against threats are the major issues. When sensitive information such as credit card number ,debit are number or any other banking information is sent then data must be protected from unauthorized access for maintaining privacy and integrity. This research paper presented different ways have presented that increases security level using cryptographic techniques.

V. REFERENCES

[1] Thomas L. Mesenbourg, "An Introduction to E-commerce", Philippines: DAI-AGILE, 2000

[2] 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

[3]D. Berlin, "Information SecurityPerspective on Intranet," presented at Internet and E- Commerce Infrastructure, 2007.

[4] 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.

[5] Joel Weise, "Public Key Infrastructure", SunPSSM Global Security Practice Sun BluePrints™ OnLine August 2001

[6] An Introduction to Cryptography (found in the documentation of PGP® Desktop 8.1). Page 17. June 2004.

[7]Jagdev Singh Kaleka, "E-Commerce: Authentication & Security on Internet", Deptt. of Technical Education and Industrial Training, Govt. of Punjab

[8] Cetin K. Koc, "Next Generation E-Commerce Security" Information Security Laboratory December 2, 1999

[9]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..

[10] 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