International Journal of Research in Advent Technology, Vol.2, No.3, March 2014
E-ISSN: 2321-9637

Analysis of Secure Electronic Transmission (SET) System for Electronic Transactions

Prof. Amit R. Manakshe[1],Mr. Saurabh Jirkar [2],Mr.Pranit Wakhare[3], Mr. Vinay Buram [4]
Asst Prof, Department of IT[1]
Department of IT[2, 3, 4]
JDIET, Yavatmal[1, 2, 3, 4]
manakshe.amit@gmail.com [1] , saurabhjirkar1616@gmail.com [2] , pranitwakhare@gmail.com [3]
vburam@gmail.com[4]

Abstract— In this paper, we introduce about protection of electronic payment for those whoever uses Internet transaction. This system is use to secure Internet transaction for three types of participants, 1) Payment gateway server, 2) Merchant server, and 3) Bank Server. SET has been developed by both Visa and MasterCard, as a way to secure our card transactions over internet, and industrial interest in the protocol is high. The security architecture of the system is designed by using Many Security Protocols and techniques, which eliminates the fraud that occurs today with stolen credit card/debit card payment information and customer information. Electronic commerce involves the exchange of some form of money for goods and services over the Internet but today, Internet is an insecure and unreliable media.

Index Terms- SSL/TLS and SET Protocol, symmetric & asymmetric Methodology, Dual signatures, and Communication tunnel techniques, e-payment protocol.

1. INTRODUCTION

Today online shopping is not new idea for us by card, because every human watch for their ease. Nowadays, everybody is depends on electronic payment, for the sake this, visa and MasterCard has developed the techniques and methods for ease of purchasing and selling products over the internet. And this idea has helped in the growth of e-payments and e-commerce services, which are very much convenient and efficient ways to do successful financial transactions.

Electronic payment involves six methods: - financial edit, electronic fund transfer (EFT), smart cards, credit cards, digital cash and online stored value systems.We are going to talk only about payment is made by the credit card/debit and the goods need to be shipped physically, whatever we want to buy.Electronic commerce involves the exchange of some form of money for goods and services over the internet but internet is an insecure and unreliable media. We focus on the following e-commerce scenario: a customer wishes to purchase goods online. E-commerce protocols have to address standard requirements such as confidentiality of information, integrity of data, cardholder account authentication, and merchant authentication. The new predicates are scalable that are used to check gradient properties of different e-commerce protocols.

A considerable need for secure and efficient payment systems that can operate over internet has been created. Most people have tried at least once or twice to purchase something online. purchasing online, whether services or products, requires that a customer have a valid credit card or international debit card or finance account such as pay pal but most online purchases use credit cards

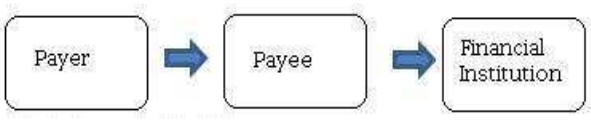

Fig. 1**:** Scenario for E-Commerce.

As shown in figure 1, all the payers are stick with communication links. In order to buy something they want, the payer needs to exchange certain information/data over those connections

If the information/data is sent over the connection in simple text (means without any encryption key), there is a possibility of eavesdropping. Whoever accessing to the network traffic, might gain access to personnel information, such as card numbers, card type, whole detail of card holder and passwords. Credit card-such as a Visa or MasterCard, has a spending limit based on user's credit limit. Debit Cards, removes the amount of the buying item from the cardholder's account and then transfers it to the seller's bank.

In e-payment system, server stores the records of every transaction. When the e-payment system automatically goes online to communicate with the retailers and the customers who can deposit their money and then the server updates these records for audit purpose.

We review Secure Payment System for Electronic Transaction. Secure electronic payment system uses different cryptographic algorithms and techniques to achieve: privacy, integrity, authentication and non-reputation.

Here we are discussing some important security requirements and attacks which then e-payment system must warn about removing or avoiding them. By discusses some of the existing secure system, how those systems work, their merits and demerits. We clarify comparison with all existing solution, finally concluded our paper.

Traditionally formal methods and software testing have been seen as rivals. Formal methods are a combination of a mathematical or logical model of a system and its requirements, together with an effective procedure for determining whether a proof that a system satisfies its requirements is correct. There are several different formal methods for analysing the protocol security, detecting protocol failures, and designing secure protocols.

2. BACKGROUND & RELATED WORK

With the increasing impact of intangible merchandise in worldwide economies and their immediate delivery at small cost, traditional payment systems tend to be more costly than the modern methods. Online processing can be worth of value smaller than the smallest value of money in the manual world. However, there are two methods of running e-payment systems.

1.Online payment: in which vendor checks the payment send by purchaser with a bank before serving the purchaser.

A**.** Payments by transaction method: in which single payment does not need previous arrangements between purchaser and vendor.

B.Payments by account method: in which purchaser and vendor should have system account with bank and certain type of agreement between both before carrying out the real payment transaction.

The payment by transaction can further be divided into two subgroups.

I. The credit card payment transaction: is tailored for large charge payment of some hundreds or even thousands of dollars. In contrast, net money transaction is usually low value payment with difficult transaction cost and online features, similar to the thought of the e-payment transaction. The drawback of the credit card payment transaction is the fee of transactions, particularly from the perspective of the vendor that have to pay some invoices to the clearing house according to the contract agreement with them. This certainly will have straight impact on the cost policy and the interest between the possible users.

II. The e-payment by small value transactions on service: This is acquiring certain interest from the area of research. A number of important services of e-payment are e-publishing and multimedia service. In these services, due to the small transaction amount, the merchant acquires relatively shopping mall revenue from every transaction.

As a result, expensive calculations such as digital signature should be limited in order to reduce the investments in software applications. In the recent years, e-payments offering a relatively key improvement in the online revenue malls. The foundation of e-payments is to take benefit of the high level of viewers by present content for a low price. Other alternative of this thought is to rating fractions of cents for equally fractional contents sums. The main features in e-payment protocol are less charges of payment amount and high occurrence of transactions on the e-commerce system.

3. SECURE E-PAYMENT PROTOCOL

An e-payment process is a sequence of actions that consists of a business work. There are two important kinds of payment transactions: i) Atomic payment transaction-single payment transaction and single payment and ii) Individual payment transaction-single payment transaction and multiple payments. Usually, an individual payment transaction consists multiple atomic transactions. Each atomic transaction supports the traditional ACID properties and must either fully commit or fully rollback.

However, the classical ACID properties do not hold when a single payment transaction involves multiple atomic payments, especially when a failure occurs in any atomic payment transaction. Since atomic transactions use a two-phase commit protocol, a coordinating process is required to manage and synchronize the composite e-payment services within a given payment transaction.

For example, consider an assemble payment transaction. An organization/company has to pay Ethiopian Birr 10,000 for electricity board, Birr 20,000 for Telephone Office, Transports office-Birr 10,000 and Birr 4,000 to Water Board. At the time of issuing a debit instruction using e-check payment instrument with Birr 44,000 assume that by the time the e-check is cleared, the last date for payment towards Water Board is over and the organization has to pay a penalty of Birr 200.

Since the balance after the two payments is not sufficient, it is not possible to transact the water board payment. Though, the payment instruction toward the electricity and telephone was successful, the complete transaction has to roll back due to insufficient amount. This complete reversal based on nothing-or-all protocol may in turn lead to late payment to other successful utility services. Hence,

the nothing-or-all protocol as described above is not sufficient to handle composite e-payments. It can result in loss of confidence and trust in the e-payment services.

Payments on the internetcan refers to either the particular type of electronic money which consists a software product or to electronically accessed products (via. a card reader and a computer), or to both of these. Systems are also emerging that will allow the use of electronic (prepaid) money to be used over a network, by allowing the cash balance of the prepaid card to be drawn in accordance with the value of the goods or services purchased. This "electronic" payment system is normally maintained or controlled by the Central Bank of a country. There is no physical exchange of money; the Central Bank makes adjustments in the electronic accounts of Bank A and Bank B, reducing the amount in Bank A's account by $100,000 and increasing the amount of Bank B's account by the same.

4. THE IMPORTANT SECURITY REQUIREMENTS OF A SUCCESSFUL SECURE PAYMENT SYSTEM

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 comfortable that they are communicating with the party with whom they think they are communicating. Applications usually perform authentication checks through security tokens or by verifying digital certificates issued by certificate authorities. Cryptography can help establish identity for authentication purposes.

1. DATA CONFIDENTIALITY (SECRECY)

The protection of data from unauthorized 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.

2. NON-REPUTATION

It provides protection against unauthorized by one of the entities involved in a communication links and having participation in all or part of communication.

3. ACCESS CONTROL.

Avoiding of unauthorized use of a resource (i.e., this service controls that unauthorized data, whoever can have access to a resource, under what those accessing the resource and what conditions access can occur are allow to do so.)

5. DATA INTEGRITY (ANTI-TAMPERING)

Secure electronic payment system consists of four system participants (segments). The communication between the participants goes through secure communication tunnels.

1. SECURE COMMUNICATION TUNNEL

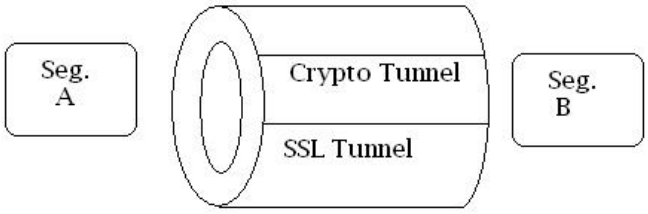

Fig. 2: Secure communication tunnel consists of SSL and nested crypto tunnel.

Secure communication tunnel consists of SSL and nested crypto tunnel, which is created by employing cryptographic algorithms and techniques on the information that are transmitted between parties.

5.2. WORKING OF TUNNEL

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

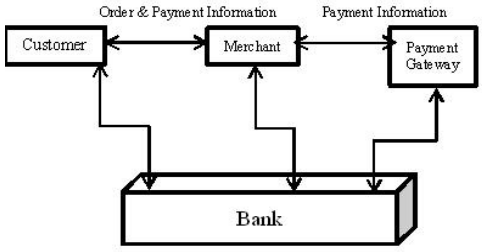

Fig. 3: Secure Communication tunnels between Customer, Merchant and payment gateway.

6. CONCLUSION

Secure E-Payment technique through SSL; secure communication tunnel and SET have been discussed in this paper. The security techniques/methods are used to provide security the customer able to purchase the desired items. The system can ensure the security of transaction, so that it becomes an excellent solution to the E-business model or any other online payment model. Main merit of Payment System for Internet Transactions are: the shopkeeper is prevented from seeing payment information; the payer can easy to use the system; it uses strong cryptography and authenticity checking models, since he is not required

to install additional software for secure payments or to have a digital certificate.

The literature shows that with the security techniques/methods for secure communication channels, a sufficient level protection provided to unsecure communication link/network.

REFERENCES

[1] Yin, Y. "The RC5 Encryption Algorithm: Two Years On." Crypto Bytes, winter 1997.
[2] ELECTRONIC CASH AND SET, Paper presented at the conference: Internet Crime held in Melbourne, 16-17 February 1998.
[3] Yin, Y. "The RC5 Encryption Algorithm: Two Years On." 1997.
[4] Gary C.Kessler, N.Todd Pritsky,"Internet Payment Systems: Status and Update on SSL/TLS, SET and IOTP" Information Security Magazine August 2000.