GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 9, Issue 6, June (2021)

APPLICATION OF SECURE ELECTRONIC TRANSACTION PROTOCOL IN ELECTRONIC PAYMENT SYSTEM

Shonazarov Soatmurot Qulmurodovich
Teacher, Department of Applied Mathematics and Informatics, Termez State University,
e-mail: sshon1989@mail.ru

Bozorov Asqar Khaitmurotovich
Teacher, Department of Applied Mathematics and Informatics, Termez State University,
e-mail:asqarbozorov1990@gmail.com

Xolliyev Faxriddin Boxodirovich
Teacher, Department of Applied Mathematics and Informatics,Termez State University,
e-mail: surxon88@bk.ru

ABSTRACT

Security of payments is the top-notch priority for every business. But payment security becomes more important when you are using an electronic payment processing system into your business. There are many security measures and protocols for securing your payment systems. Electronic payment is very important the stage of the electronic business system and the need for its security
secured.Secured electronic transaction means providing online credit card payments that are discussed widely in the pratokoli. Because of a set of implementation issues have not really been taken up by despite the fact that it is e-commerce participants
does not solve all security issues, but SET. SET the x.It is based on 509 standard certifications. This standard is the most reliable type of protection on the Internet so far, through the entire head of the theme we will come out

Keywords: Secure Socket Layer (SSL), Secure Electronic Transaction (SET), Search for a solution, Solution Search Results, Provide Authentication.

INTRODUCTION

Secure electronic transaction (blockage) was the first communication protocol used by e-commerce websites to secure electronic debit and credit card payments. A secure electronic transaction has been used to facilitate the secure transmission of consumer card information through electronic portals on the internet. Secure electronic transaction protokols were responsible for blocking out personal information from card information, thus preventing traders, haskers, and consumer information from entering the hands of electronic thieves to prevent secure electronic transaction bratokoli, SET. SET the x.We will look at the 509 standard as an example.
The research reported here builds on the electronic payment security; we study the security of e-commerce protocols and we propose a new efficient protocol to ensure a high security for electronic payment transactions.

MAIN PART

The issue of security in banks and electronic payment systems is radically different from the security of an organization or corporate network. This complexity consists of common threats as well as difficulties in creating convenience for bank users and users of electronic payment systems.

In addition, the fact that information in organizations and enterprises is considered a necessary information in a narrow range also reduces the threat to this information. This is not the case with electronic payment systems or banks.

The following should be taken into account when ensuring information security in banks and electronic payment systems:

1. Information in banks and electronic payment systems is associated with real money. This can result in serious financial damage due to stolen data or altered data.
2. That the information in banks or electronic payment systems belongs to customers. Every bank or electronic payment organization must keep this information confidential. The emergence of threats, in turn, leads to the departure of customers from this organization or bank.
3. Nowadays, the widespread use of the Internet in our lives allows you to remotely separate the work in each area. In turn, banks have the opportunity to make remote money transfers.
4. Information security in banks and electronic payment systems should be high. This is necessary to store bank or organization information on the one hand and customer information on the other.
5. The storage of information in banks that is valuable to customers and the interest in this information by many other intruders.

Crime in banks has the following characteristics:

- Confidentiality of information on crimes and threats currently available in banks. The reason for not declaring a crime is not to worry customers and not lose their position as a result;
- As usual, the intruder can use his account and most of the intruders do not know how to hide the stolen money.
- Many computer crimes are financially minor. The damage from them ranges from $ 10,000 to $ 50,000.
- The need to perform many (several hundred) steps to commit a successful computer crime. Can do a lot of things when transferring large amounts of money.

The following two main tasks are set in ensuring information security in electronic payment systems.

1. Analytical task. This task involves planning or analyzing accounts. This task is not considered operational and can therefore take a long time, and the result clearly affects the relationship between the customer or the project and the bank. Therefore, this task should be separated from the basic information processing process. Powerful computing devices are not required to perform this type of task, averaging 10-12% of the total device and equipment. An important aspect is the constant performance of this task.
2. Daily task. These tasks are performed on a daily basis and consist primarily of making payments and correcting the account. Exactly this process requires the main resource of the system. Because each transaction is completed in a short period of time, the account number,

amount of money or customer confidential information must be kept strictly confidential during this process.

TYPICAL TASK.

SET is based on X.509 standard certifications. This standard is currently one of the most trusted types of protection on the Internet.

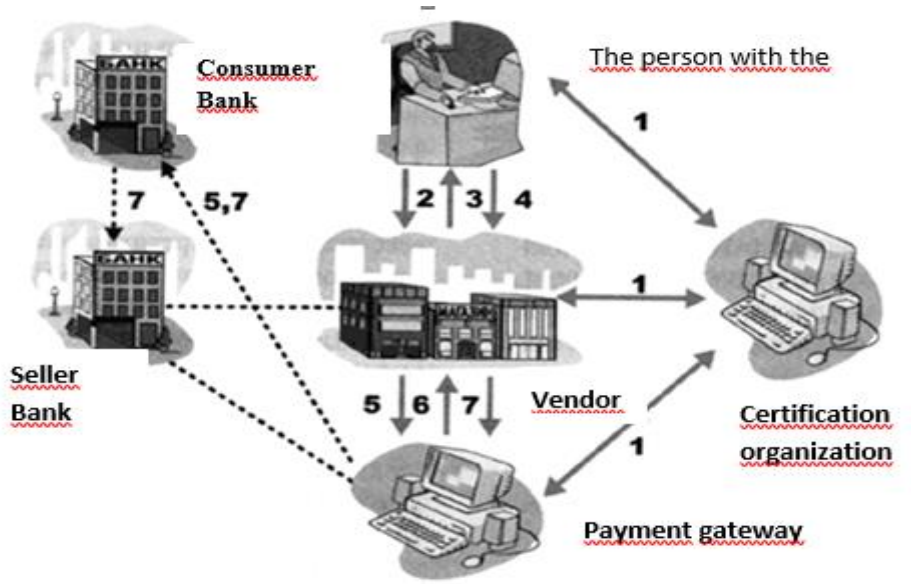


Figure 1. The structure of the payment system based on the SET standard

DECISION

Pictured above:

- Buyer with a card;
- consumer bank - a financial institution that provides a credit card to the consumer;
- Payment gateway. The system that manages the seller's bank, processes the request from the seller and submits it to the buyer's bank.
- Certification organization - consists of parts of the organization issuing and inspecting the certificate.

The sequence of processes in the figure above is as follows:

1. Participants (consumer, seller and payment gateway) receive a certificate from the certification body.
2. The plastic card holder selects the desired product or service from the online store and places an order with the seller.

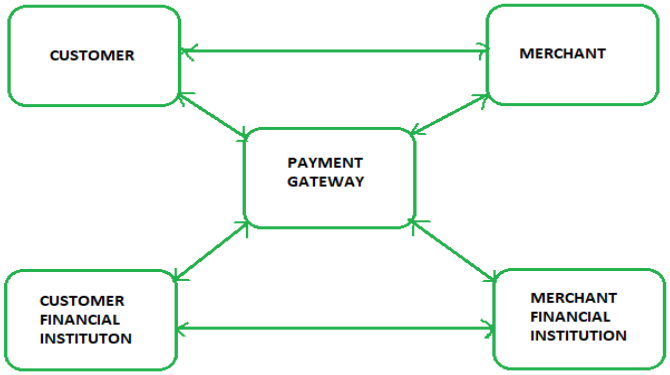
- The seller shows his certificate to the consumer.
- The consumer shows his certificate to the seller.
- The seller sends a request to the payment gateway for the actions to be performed. The gateway compares the information provided and the information received from the bank.
- After checking, the gateway sends the result to the seller.
- After some time, the seller asks the gateway to perform one or more banking operations. The gateway sends a request for a money transfer from the consumer bank to the seller's bank.

RESULTS AND DISCUSSION

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let's see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution.



CONCLUSIONS

Payment authorization as the name suggests is the authorization of payment information by merchant which ensures payment will be received by merchant. Payment capture is the process by which merchant receives payment which includes again generating some request blocks to gateway and payment gateway in turn issues payment to merchant.

REFERENCES

1) Hassler, V. (2001). Security Fundamentals For E-Commerce. Artech House, Massachusetts.
2) G. Dhillon, J. Ohri, Optimizing Security in E-commerce through Implementation of Hybrid Technologies, CSECS'06 Proceedings of the 5th WSEAS International Conference on Circuits, Systems, Electronics, Control & Signal Processing, Pages 165 – 170.
3) Z. Jiemiao, Research on E-Payment Protocol, Information Management, Innovation Management and Industrial Engineering (ICIII), 2011, pages 121 – 12.