IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. III (Jul.-Aug. 2016), PP 92-94
www.iosrjournals.org

Security in E-Commerce

Maryam KeshtkarYamini
Computer software Engineering, Payam Noor University of Qazvin

Abstract: *Despite the all benefits of e-commerce, the transaction and online connections provide a great space for the abuse of technology, even the criminal acts.The organizations should find out a security system, tailored to their needs and apply it.Although the service selection, tailored to the various sides of organization, is a difficult act, but the experts, the custodian of selection, implementation and organization of security information systems, should evaluate the available options accurately and choose the best one.*
Keywords: *digital money, Secret signature, coin transaction*

I. Introduction

In nowadays developing world, the half of our life events occurred in virtual world.Data transaction, download and upload of sound and visual files, secret information, the bank account checking, sale and purchase of goods and lots of the other actions take place in virtual space of Internet.In modern world the old form of doing works has been changed and the commerce is no exception of this rule. The new form of commerce is e-commerce. Investment, electronic marketing, e-payments, online stores, on sale great markets and … are the parts of e-commerce wide domain. In new systems the security concept is widely presented and the information security systems should be applied as the information security to provide the security in both physical and informational sides.

II. Digital Money Security

Memorizing a password for credit card was replaced of paper and physical money. But the e-money could not bring the needed security. Because the hackers threat the electronic accounts every day via a new trick. The digital money security presents a novel payment tool in e-commerce. Some selected mechanisms for the digital money transactions in full security have been presented below.

1. Undetectable Payment transaction

When you take money from ATM, their serial number is not recorded, therefore the done transaction could not be related to an especial customer. Digital coins have the individual serial number, so it is easy to record a list that every serial number dependency to customers. Looking these numbers, it is easy to detect the transactions of individual customer. Prevention of this action, especial mechanism will be needed in e-commerce.

1-1. Secret Signature

Using this mechanism, the relation between coins and the client identity will be vanished. This mechanism is based on RSA or Secret Signature.

1-2. Exchange Coins

Unknowability of payer and undetectable payment transaction in this mechanism is provided based on reliable third person.Reliable third person is an organization that both sides have reliability on it. There is a network of money servers that changes the identified coins with undefined coins after the validity confirmation. This kind of anonymity is weaker than secret signature.

2. Coping with Double Payment

Digital coins can be copied easily by everyone because the electronic numbers are simple. If a payer earn a coin legally, he/she can consume it more than once that is illegal, therefore some mechanisms should be to prevent the second consume of coins.

2-1. conditional anonymous via the selection and cutting

Conditional anonymous mechanisms are activated just for the cheating clients. While the honest clients will be anonymous but the identity of cheater clients who try to spend a coin double, will be disclosed.

2-2. Secret Signature

In systems based on secret signature, the all coins serial numbers should be saved that caused the huge amount of work and scales. This system only is suitable for the online payment systems because the data base is assessed every time that payer spends a coin.

2-3. Exchange Coins

To cope with unknown user, the coin exchange can be done in a safe money server. For this reason only the serial number of coins that have not been spend yet, saved in money server and if a coin consumed the related serial number will be eliminated from the total list. Therefore this procedure will be able to do huge amount of works and high scales, comparing the previous procedure. In this procedure the anonymity is weaker comparing the secret signature procedure because at least one money server should be confirm by user. This system only is suitable for the online payment systems because the data base is assessed every time that payer spends a coin.

2-4. Guard

This mechanism is used for the coping the double spend of a coin in offline system. The exporter is a bank organization which export electronic money. Wallet contains the money and guard that money wallet and the guard confirmed by the payer and exporter respectively. The guard is a microprocessor which put into the wallet or attached on a credit card and its role is to protect of exporter benefits during the offline transaction. Indeed the guard prevents the extra spend r double spend.

3. Dealing with Counterfeit Coins

Generally counterfeiting the classic coins is quite difficult. At first the signs should have the special physical properties that their production is difficult and expensive, also the serial numbers should be appeared original. The serial numbers can be checked in validate exporter resource and detectable.In online systems the serial numbers can be checked before the payment but it could not be extended to huge works and it is not performable. Only choice is the coin exporting with serial numbers which have the especial mathematic properties. Actually the costly coin production in coins with low value is not affordable at all. Micro Mint as an offline payment credit system believes that the cost of one coin production in high volume is fewer than a few coin production. This action is performed by the Hash functions.For the security rising in this situation it is possible to limit the coin validation by time duration.

4. Deal with Coin Theft

An individual way for coping to digital coin theft is the cryptography. But the coins have low value therefore in many cases the cryptography mechanism is not enough and expensive.One solution is the custom coins using that contains the client version and salesperson version. Actually coin customization creates some limits for the clients. A simple way for the coin customization is the adding of client identification information. However in some cases the clients prefer that coins be without name because of the coin missing risk. In such cases the theft probability will be decreased. For this type of coins, the client must connect with online inductor every time that face with new type salesman. The protocols are designed for the 50 cents purchases for electronic information buying such as online newspapers, magazines or investments. In this method, the inductor is the most reliable part and therefore it should be a reliable financial institution such as a bank. If the clients and salesman co-operate to each other, they can determine the inductor in case of violation. Explained model is based on three boundary:

Master Customer Secret:

For the customer-secret obtaining, the information of customer in scrips used. Customer-secret is used for the scrip owning confirmation. Master-customer-secret is calculable based on Hash with client identity variables. Also master-scrip-secret is used by the salesman for the prevention of tamper and counterfeit.In presented sketch by Millicent, the scrip is addressed to the digital coin. Scrip has the low value and can be spend by the customer ID. Therefore the scrip belongs to customer and salesman. Scrip consists of body and a license. The scrip body consists of below cases:

- ✓ Seller, price, expired date, customer properties
- ✓ Scrip identity
- ✓ Customer identity
- ✓ Serial number

If the scrip sent obviously, there is theft probabilityeven it belongs to client individually. For example an eavesdropper can use the scrip with copying the changed scrip. The purchase protocol is as below:

- ✓ Customer to seller: scrip, request, Hash function, request and customer-secret.
- ✓ Seller to customer: changed scrip, response, Hash function, License, response and customer-secret.

This protocol has the best efficiency in security consideration in transactions between the whole Millicent protocols. Customer ID of changed scrip is the customer ID scrip that export via the customer message.

Security Strategy

The security implementation strategy consists of below steps:

1. Host security
2. Operation system security
3. Web server security
4. Network security
5. Antivirus tool
6. Firewalls
7. Security Policy

Types of attacks based on performance way: Interruption, Interception, Modification and Fabrication.

III. Conclusion

The way of payments and security should be paid attention by marketers. The serious attention of marketers to payment ways maybe caused the profitably and costs decreasing. In security case this is so important to say that if the marketers don't have security so they can't deal easily.

References

[1] Daniel L.Ruggles, IT Solutions Series: E-Commerce Security: Advice from Experts,Cybertech Publishing, 2004,
[2] Hassler, Vesna, Security Fundamentals for E-commerce, Artech House on Demand Publishers, 2001