The Analysis on Electronic Business Online Payment Security Technologies

Qing CHEN*, Fang WAN

Institute of Technology, East China Jiaotong University, CHINA
*s021713@163.com

Keywords: Electronic commerce; Online payment; Security risk; Optimization measures.

Abstract. With the rapid development of economy and technology, e-commerce transactions have walked into people’s lives. Although online payment can save time, it has some problems at the same time. How to do a good job of e-commerce online payment has become an urgent problem in modern society. This article will explore and analyze online payment security system, the technical risks of the online payment system, the security risks and the related optimization measures.

Introduction

In China, online-payments account for a large proportion in shopping, which not only bring convenience but also exist security problems at the same time. Some lawbreakers take advantage of the advanced technology and the security of e-commerce transactions are not guaranteed and confronted with risks. This article will explore the online payment security system, the technical risks of it, the security risks faced and the related solutions, aiming at further improving the electronic commerce payment security technology.

E-commerce Online Payment Security System

Online payment is one of the most important parts of E-commerce. In general, data encryption and identity authentication will be used in online payment, which makes the electronic trading environment more reliable and allows users to consume more safely. The below is the brief introduction of online payment security system, including the following aspects.

Network Payment Security Protocol

There are two kinds of secure online payment protocols widely used in network payment. One is Secure Sockets Layer protocol, and the other is Secure Electronic Transaction protocol. The two protocols can provide three basic security services. The first is confidentiality. There is a cryptographic algorithm and key agreement between the client computer and the server system. Through this negotiation, a secure channel is established and all the information passing through the channel will be encrypted. Some lawbreakers who want to get the information will eventually get useless cipher text. The second is integrity. Secure Sockets Layer protocol uses cryptographic algorithm and hash function to ensure the integrity of the information by extracting the eigenvalues of the transmission information. Therefore, all information can be completely transmitted to the final destination. The third is authentication, which uses certificate technology to allow the client computer and server to identify each other. In general, the Secure Sockets Layer will exchange digital certificates with the user when the certificate holder is a legitimate user and ensure the legitimacy of the identity of the two.

Encryption Technology of Secure Sockets Layer for Online Payment System

With the basic Secure Sockets Layer protocol, both ends are encrypted. Firstly, the digital authentication certificate should be bought and installed and then get the service content and scope of the payment gateway from the online payment service provider. Generally speaking, the user will choose a credit card transaction and a transaction processing system. The transaction processing system will also be different as different digital certificates are purchased from different companies.
Implementation of Payment Function and System Integration

In order to realize the whole process of online payment system, codes need to be written in the function page and the interface parameters should be defined according to a specific specification to complete the payment process. It needs to be integrated into the system after a transaction type and a transaction processing system are selected. The first step is to do the safe connection between the server and the client computer according to the selected transaction mode; the second step is to take a reasonable way to safely acquire the relevant information of the customer; the last step is to submit the credit card and address information to the payment gateway for verification based on a specific format which is to define the input and output interface parameters. Thereafter, the codes will be added after the parameters are defined. After the series of procedures are completed, the payment gateway shows the result of user authentication as passed and the user can then pay the transaction. If the authentication is not passed, then the customer can enter the correct information according to the message.

Technical Risks of E-commerce Online Payment System

From the above, it can be seen that e-commerce online payment system mainly includes network payment security protocol, the Secure Sockets Layer encryption technology of online payment system and the realization of payment function and system integration. Next, the technical risks of E-commerce online payment system will be explored from the following aspects.

The Reliability of the Payment System is Low

With the increasing scale of e-commerce, there appeared many protocols to ensure the security of electronic commerce payment system in China. But people are still suspicious about whether these agreements and the existing technology can truly guarantee the security. Unlike the traditional way of purchase which is in written forms and cannot be easily altered, the electronic payment of the online banks is not guaranteed by the written certificate. This requires that a good job in the security of data transmission in technology should be done to ensure that the data will not be stolen and tampered. In China, many banks have introduced various measures to tackle unsafe factors to further improve security of e-business online payment. At the same time, there are fraudulent behaviors in society, but the appearance of third party payment makes the probability of fraud decrease.

Nonstandard Safety Certification Authority Increases Risks of Online Payments

The prestigious China Financial Certification Authority was established jointly by The People’s Bank of China and other commercial banks. As an authentication institution, it can require users to provide relevant information of authentication and at the same time, it can check the use certificates at any time. Certificate mechanism guarantees the information authenticity, integrity and privacy, which can further ensure the security of electronic business on the internet to a certain extent. However, in China, it lacks unified authority legislation to regulate the market access mechanism, operation procedures and etc. The absence of effective supervision will lead to insufficient trust of the users toward the payments.

Security Risks Facing E-business Online Payment

From the above, it can be seen that the lack of trustworthiness of payment system mainly lies in increased risks resulted from the lack of security of payment system and nonstandard security authentication. According to these information, there is more understanding of the security risk facing the e-business online payment. Next, the security risks faced by e-business online payment are analyzed mainly from the following aspects.
Alien Attacks

Users will lose control of their accounts due to alien attacks. In general, there are three kinds of alien attacks which include phishing scam, computer virus and computer hackers. The first is phishing scam, which is common in China. Generally, unlawful criminals use counterfeit emails and websites to cheat users. For example, the criminals imitated a bank's website and then deceive users into logging in the bank card's account and password by telephone and withdraw the user’s money from bank account. The counterfeit websites are similar with the real websites and it is easy for users to get trapped. The second is computer viruses. Many kinds of viruses have been found in the world for online banking services. If the viruses invade the user's computer, they will exist for a long time. When users use this computer for online banking and other services, the user's account, password and other information will be automatically recorded and then sent to a designated site through a channel, making the user's online bank data stolen, causing greater losses to the user. The third is computer hacker. No matter how advanced technology is developed, there is no fully secure physical network system. Computer hackers master a lot of technology and they focus on attacking websites. They may revise the information of the online banking database so that the users' funds are directly converted to them, which is also a great loss for the users.

Electronic Money is a Direct Target

Electronic payment has a wide range of applications because of its convenience, and for this, many criminals will commit crimes. Criminals take advantage of the convenience of electronic payment and set their goals as funds in the user's network bank account. A lot of news and cases about funds transferring from the users’ account are heard. Sometimes criminals can also induce the users to make bank transfers by message fraud or the information of the bank's Automatic Teller Machine. Many users will be deceived and suffer greater losses.

Main Reasons

There are three main reasons for the accident of online payment. The first is the user's weak sense of security and the lack of privacy awareness to easily disclose their account and password and other important information to others. During online payment, there is no correct identification was made or no anti-virus software was installed in the user’s computer, or the version was too low to attract some lawbreakers’ attention. The second is the electronic payment security problems. Bank transfer errors may happen due to wrong operation and so on. Or it may also be caused by hackers attacking computer and viruses. The third is that the legal liability of electronic payment is not clear as China currently lacks special laws for the security of electronic commerce. If there is a delay in payment or a payment error, it is also a big social problem on who will take the responsibilities: the trading parties, banks and authentication authorities. The lack of specific legal provisions may lead to the phenomenon of buck passing among the three parties.

Optimization Measures for the Security Technology of Online Payment

From the above, the security risks faced by e-business online payment mainly include alien attacks, the direct target of electronic money and the main reasons. According to the above information, the scientific and rational online payment security technology for e-commerce are put forward in the following.

Establish and Improve the Legal Mechanism

From the beginning of 2013 to 2014, China had formed an outline of the legislation on e-business. The beginning of the draft law was completed from 2015 to 2016, embodying the formal start of the legislation work of the electronic business in China. China has also been constantly thinking and analyzing e-business law, and further improving the relevant laws. The establishment of a sound law could solve problems in accordance with the provisions of the law and avoid other problems arising from the buck passing.
Perfect the Network Information Security Technology

Modern network security will adopt digital certificate and encryption technology. The encryption technology uses the Secure Sockets Layer protocol. In this protocol, the two encryption methods of public-key cryptography and private-key cryptography as well as the secure Electronic Transaction will be used. Technologically, encryption researches will be made and continuous upgrading of technology can also make it impossible for criminals to take relevant measures to solve. For digital certificates, it is necessary to take security measures. The contents of the digital certificates mainly include the original fingerprint and password, and the mixed authentication and human biological recognition can also be used, which can greatly improve their security.

Build a Perfect Personal and Enterprise Credit System

The government has to strengthen the level of personal and credit. Firstly, a good job of credit publicity and user guidance should be done. Secondly, relevant measures should be made. For those users with poor credits, punishment or other measures should be adopted, which will make users pay more attention to their own information and can further reduce the probability of crime to a certain extent.

Strengthen the government's supervision

The government departments should make full use of the existing platform to carry out propaganda and enhance the supervision of financial institutions and enterprises in the society. The regulation should also depend on relevant rules and regulations, which can further improve the security technology of e-business online payment.

Conclusion

To sum it up, the article makes explorations about the security technology of e-business online payment. The main optimization measures are to establish and improve the legal mechanism, improve the network information security technology, build a perfect personal and enterprise credit system as well as increase the government supervision. E-business online payment accounts for a great proportion in our life and the relevant departments must ensure their security in order to promote the further development of e-business. At the same time, it will also greatly boost China's economy and science and technology.

References

