Analysis the Development and Security Policy of Third-Party Online Payment Platform

Chenggang Zhen  
Network Administration Center  
North China Electric Power University  
Baoding, China  
zhencg@163.com

Peng Cheng  
College of Computer Science and Technology  
North China Electric Power University  
Baoding, China  
wolfpkwolf@163.com

Abstract—Online payment is the key point and the basic conditions to the development of electronic commerce, which greatly promote the development of e-commerce, and brought prosperity to the e-commerce. As e-commerce is one of the fastest economic growth of China, the online payment and its security becomes particularly important. This paper analysis from three aspects: the current development status of e-commerce online payment in China and its main ways of payment, as well as the existing problems. And combined the actual situation in our country, raised the foundation of e-commerce third-party online payment platform, especially, raised a new perspective: Design and develop the payment software for client-side as well as integrated planning the third-party online payment platform, in order to establish the unit and rational interface which can match the payment software for client-side. Make sure the security of the online payment transactions can be achieved.

Keywords- online payment, security policy, information security, transaction security

I. AHEAD OF THE TRADITIONAL ECONOMIC GROWTH OF CHINA'S INTERNET

Ten years ago, shopping online perhaps still a new thing to the public, we all have more of a curiosity and doubt, etc. But ten years later, shopping online in nowadays is no longer a novelty; we all ask that whether you go shopping online? Yes, in today's opinion, shopping online is already a very common thing in our daily life. According to the survey data, it's a potential for the shopping online of the e-commerce.

A. Market size

Sub-sectors in e-commerce market has a great potential

TABLE I. THE COMPOUND ANNUAL AVERAGE GROWTH RATE AT DIFFERENT TIMES OF CHINA'S SUB-SECTORS INTERNET.

<table>
<thead>
<tr>
<th>percentage (%)</th>
<th>2004-2008</th>
<th>2009-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shopping online</td>
<td>35.8%</td>
<td>62.1%</td>
</tr>
<tr>
<td>Search engines</td>
<td>76.2%</td>
<td>48.2%</td>
</tr>
<tr>
<td>B2BE-commerce</td>
<td>76.5%</td>
<td>36.9%</td>
</tr>
<tr>
<td>Interne teconomy</td>
<td>47.5%</td>
<td>35.30%</td>
</tr>
<tr>
<td>Online game</td>
<td>59.0%</td>
<td>33.9%</td>
</tr>
<tr>
<td>Onlinerent</td>
<td>35.4%</td>
<td>31.0%</td>
</tr>
<tr>
<td>Travelreservations</td>
<td>47.7%</td>
<td>29.5%</td>
</tr>
<tr>
<td>Brandnetworkadvertisements</td>
<td>62.8%</td>
<td>28.8%</td>
</tr>
<tr>
<td>Mobile Value-added</td>
<td>29.5%</td>
<td>22.1%</td>
</tr>
</tbody>
</table>

According to the above analysis, we can see that the compound annual growth rate of shopping online is the highest in 2009. According to the news of December 30, 2009, IResearch sought advice from analyst Jiang Lixin to say again recently released the report about the data of online payment in 2009. This report has shown that the transaction size of annual online payment has reached 576.6 billion yuan, doubling for five consecutive years. In the period of 2005-2009, the transaction size is increased by nearly 30 times.

In 2009, now its 11th year of China's online payment development. Online payments continued strong growth, the transaction size reverses a growth continuously in five years. It will reach to 576.6 billion yuan in 2009, and the expected growth rate is about 110.2%. The rapid growth of subscribers is also increased. Compared with the 52 million in 2008 and the growth to 90 million, the growth rate has reached to 73.1%. IResearch expects that the transaction size of online payment will exceed 2 trillion, and it has a very bright future. Online payment has become a star of Internet industry.

B. Users scale: the scale of the online payment users have reached to 90 million.

IResearch seeks advice from predicting that in 2009, the users scale of online payment in China will reach to 90 million(used at least once half a year), compared to the 52 million in 2008 increased 73.1%. The penetration rate of net citizen will reach to 23.1%, compared to 2008 is expected to increase by 5.7 percentage points.
The growth rate of online payment industry in 2009 exceed the IRResearch seeks advice from predicting before the year. This reflects that the strong growth industry. IRResearch forecasts the transaction size will exceed 2 trillion yuan. According to the 0.5% rate of return (revenue/turnover) estimates, then the scale of revenue size will exceed 10 billion yuan.

The optimistic expectations of IRResearch for the following reasons:

Firstly, the proportion in the third-party online payment transactions of the community is still low, and in the future, the proportion of the e-commerce payment will increased, while the third-party online payment operators is the most competitive part in the chain of e-commerce payment industry. Secondly, the current e-commerce to some extent changed the business environment in China, and in the future this kind of change will continue, but the next five years is the period of initial success and continue to advance; Thirdly, Online payment for now is more healthy competition, cooperation with the chain of industry more closely, it can create value for the many ways.

Huge opportunity, and carries a huge profit, but also nurtured a great danger. The development of online payment in nowadays has formed a certain scale, and the future market with huge potential, but with this discovery is the biggest threat from online payment security issues.

II. THE CURRENT SITUATION OF THIRD-PARTY ONLINE PAYMENT

The so-called third-party payment is that some major banks at home and abroad signed a contract to provide the interface of various bank cards, and possess the necessary banks at home and abroad signed a contract to provide the industry. Secondly, the current e-commerce to some extent in nowadays has formed a certain scale, and the future market with huge potential, but with this discovery is the biggest threat from online payment security issues. It can achieve a win-win situation with the banks. Secondly, On behalf of the Alipay—the type of credit-backed which is the third-party payment platform. The basic process of Alipay: When the buyer to payment Alipay online, Alipay received payments after the notification delivery, the buyer received the goods, and then notify the Alipay after confirm no problems with the goods. Alipay then transfer the money to the account of sellers. If there is a phenomenon of fraud behavior, the full settlement will be paid by Alipay. The third-party payment system as a type of credit-backed third-party payment platform, it not only ensure the safe transfer of funds, but also become the credit intermediary which can constraint the behavior of both sides, and eases the problem of asymmetric information, increases the credibility of shopping online.

With the rapid development of e-commerce, online payment become more and more common, and third-party payment platform has been developed rapidly. According to survey data and network IRResearch forecasts in 2004-2013 , the transaction size of third-party online payment in China as shown below:

![Image](image)

Figure 2. 2004-2013 , the transaction size of third-party online payment in China.

In 2009, Alipay reinforced the advantages of individual clients, while increasing security, enhance the experience of users, innovation and personal services, increase applications and improve the payment channels, etc. All have a better performance on the above aspects. There is a fast growth of its customers, and in the period of August 2008 to July 2009, at the time of less than a year, the registered users to add 100 million to 200 million. The transaction is expected to reach the scale of 286.9 billion yuan, and the proportion of market reached to 49.8%.

Tenpay takes follow policy, and walk out a different way of development from the Alipay. The emphasis point is in the area of aviation combined B2C sales, B2B settlement and enterprise funds clearing and settlement; and the strong point of network can be maintained.

Under the strong market structure of the Alipay and Tenpay, if the other small platforms want to be lived, it's proposed that platform for competitive differentiation, and consider with the industries, regions, users and other dimensions.
The significance of information in the modern society, the information economy and the information age. One of the main issues of information security is lack of sufficient systems’ security, reliability, standards, and communication protocols. Moreover, the software development tools are still evolving and changing rapidly. Hackers can hack the system not only for the inadequate security system but also for the basic fundamental mistake made by the programmer while designing the system. “As developers strengthen security products in response, the attacks become more sophisticated, creating an ever-escalating and quickening cycle of attack and defense”. Gauzente and Ranchhod depicted that customer service to the internet also poses great challenges, including the emergence of serious privacy concerns and resulting negative consumer responses. This kind of threat to consumer privacy posed by the internet requires urgent attention as it may undermine a firm’s marketing performance in the long run. Information is a precious asset in any organization whether it is printed or written on paper, stored electronically or by any means. To manage the threats and risks to any organization's information effectively the company needs to establish an Information Security Management System (ISMS).

2) Transaction security

The rapid growth of internet and number of online consumers has resulted in increased fears regarding the guarantees of privacy when using e-commerce. There are risks in transferring money electronically such as altering consumers' account details. In internet, the data can be accessed without physical access or presence. This facility not only assists the user but also gives advantage to the criminal. Information infrastructures connected with public network are vulnerable to various attacks from both inside and outside the organization. The risk involved in e-commerce could be the compromise of customer confidentiality, like unauthorized access to customer information, and the remote launch of denial of service attacks on a server. In all cases, the most damaging for any company or organization is the exposure of security vulnerabilities and attacks, which leads to damage of reputation and consumer satisfaction. Another possible risk association with an e-business venture is the failure to comply with requirements from a regulatory body; although this is a manageable risk unlike risks from malicious individuals. Security issues are one of the biggest barriers to internet sales growth. Young as cited by Hopwood, “Competitors are the single greatest threat in computer crime”. In addition to competitors, employee theft through e-commerce is an important issue. Disgruntled employees may wish to steal assets or sabotage the company as a means of revenge. Other employees may steal to satisfy a perceived need for cash. Purchasing on the Internet holds risks such as retailer might misuse customers’ personal information. According to McGuire, there are nine basic threats to information security which are as follows:

- a) Data destruction,
- b) Interference,
- c) Modification/replacement.

III. THE SECURITY ISSUES AND ITS CORRESPONDING SECURITY POLICY OF THIRD-PARTY ONLINE PAYMENT PLATFORM.

A. Security issue

The security issues of online payment generally can be divided into two categories: Information security and transaction security

1) Information Security.

Information security is defined by the US National Security Telecommunications and Information Security Committee as the protection of information and the systems and hardware that use, store, and transmit that information. Martin reported that, without an uninterrupted flow for this vital resource, society would quickly run into difficulties, with business and industry, education, leisure, travel and communications, national and international affairs- all are vulnerable to disruption. In more advanced societies, this vulnerability is exalted by an increasing dependence on the enabling powers of information and communications technologies. The significance of information in the modern world can be measured by the three terms: The information society, the information economy and the information age. The figure is about the market share transaction size of China's third-party online payment companies in 2009.

![Figure 3. The market share transaction size of China's third-party online payment companies in 2009.](image)

Although the third-party payment model to some extent mitigated the security of online transactions, but the internet consume complains incident as well as the account theft incident frequently be occurred, it makes people have concerns for shopping online. Now it is a wide range of network virus, a variety of ways and means of communication, threatening the security of payment platforms. One survey in U.S. shows that most online payment has three main concerns: Firstly, the security of online transactions; Secondly, the process of online payment disclosure of user information, including user information, the user credit card information; Thirdly, for now, the design to third-party online payment platform is just use the web client to achieve, and no special payment client system. Therefore, in the last place, security is still the unavoidable issue. It can clearly be seen that the security of online payment has become the bottleneck of the development of online payment. In order to maintain its current good momentum of development, security must be guaranteed.

![Figure 3. The market share transaction size of China's third-party online payment companies in 2009.](image)
Although companies are providing guarantees, still there exist two type of risk in the on-line: system-dependent risk where there is no control over the transmission of data and transaction-specific risk where data might be passed to the third parties or theft by employees. According to Van Slyke and Belanger, "the level of trust that individuals and organizations are willing to place on online purchasing is one of the most important barriers to the use of the internet for conducting business today". However, Hagel and Armstrong, as cited by Durkan, et al., “the absence of personal contact to provide some sort of tangible measure of authenticity and reassurance, combined with the unfamiliarity of the on-line environment, can lead to consumer anxiety". Raja reported that transactions in electronic commerce can occur without any prior human contact or established interpersonal relationships and this lack of interpersonal trust creates a circumstance for a security threat. Fleischer, Google’s Privacy Chief, verifies that “Three quarters of the countries in the world have no privacy regimes at all". Some companies collect information about customers’ through internet without their consent.The internal security threat covers not only the misuse of confidential information or accidental use of information outside the organization by some employees, it also includes where and how the users are accessing systems and data which relates IT helpdesk utilization, password usages and security responsibility. The different features and use of e-commerce add security threats in it because of its mobile nature . Although we are living in an information age but still some of the leading organization can not protect their customer’s important personal information. It might be for the lack of security or just the ignorance. Symantec noted that in the latter half of 2005, 80% of the top 50 reported threats could be used for data theft. May be many organizations do not understand the value of the information. In the following paragraphs some of these will be discussed as examples. In fact, data security was the most common type of financial crime incident dealt with during the year and it is highly likely that many data loss incidents go unreported". FSA said that these cases have revealed some serious weaknesses in firms’ data security.A computer printout with 13,000 mortgage customer’s account details was stolen from a member of staff in 2007 from the Halifax bank. Earlier of the last year, they also dumped customer account details in outside the bins.During the first six months in the last year slammer attack was performed by 31% of the IP addresses detected attacking targets in the financial services organization. This attack is commonly associated with three high-profile malicious code samples: Slammer, Gaobot, and Spybot, according to the Symantec Data. One of the most popular and successful techniques employed by cyber thieves to steal a person’s identity entails the use of deceptive e-mail phishing attacks. According to the latest edition of the Symantec Internet Security Threat Report, the number of blocked phishing attempts against targets in the financial services sector rose from a weekly average of 11.0 million attacks in January 2005 to a weekly average of 15.3 million in June 2005. Gartner, as cited by Butler, a reputable research organization, reported that 10 million USA adults were victims of identity theft in 2005, causing almost $15 billion in losses. Poor business practices create administrative threats in the form of password sniffing, data modification, spoofing, and repudiation. As a result most of the company is losing trust to their customer and consequently earning bad will for their company. To avoid or minimize these problems all organizations should practice an effective information security management system within the organization. Phishing is an activity, attempt by a third party to solicit confidential information from an individual, group, or organization often for the financial gain. Therefore, mainly financial services are mostly affected by this.

B. security policy

All of these days, the industry experts continue to explore the solutions and strategies of the information security and transaction security; it can be divided into the following two aspects:

1) Technical security strategy
   a) The opening tag of interests' information exchange makes the information services more fragile in terms of security, and networks have developed at all levels with the corresponding security protocols and security technologies to ensure the security of e-commerce.

   b) The security of the network platform. The common method is the use of firewall, virtual private network (VPN) technology, and anti-virus protection.

   c) The technologies such as encryption, digital signatures, and electronic authentication be expanded and applied.

   d) Online payment agreement, the SSL (Secure Sockets Layer) protocol and SET (Secure Electronic Transaction) protocol. The SSL protocol is in the network transport layer and application layer provided between the RSA and secret key based on the browser and Web server for secure connection between the technologies. SSL through digital signatures and digital certificates to implement authentication, digital certificate from the certification body (Certificate Authority, CA) obtained usually contains the name that uniquely identifies the certificate owner, the only name of publisher identity certificate, the owners of certificate, the certificate issued by the digital signature certificate is valid and the certificate serial number. The use of digital certificate authentication on both sides, both sides can use the secret key for a secure session. SSL protocol in the application layer send and receive data before encryption algorithm negotiation, key and certification of two sides of communication link, the application layer so as to provide a secure transmission channel: the channel load can be transparent to any high-level application protocol (such as HTTP, FTP, TELNET, etc.) to ensure the application layer data security. The SET protocol is an open network can guarantee the security of funds through the payment of technical standards. It uses
technology, including symmetric key encryption, public key encryption, hash algorithms, digital signatures and public key authorization mechanism. SET make the order information and credit card information be isolated. When put the orders contains the credit card number information to the merchant, the merchant can only see the order information, but do not see your credit card number information, and the need for mutual authentication of cardholders and merchants to determine the identity of communicating parties, usually by a certification center for both provide credit guarantees. SET defines a complete electronic transaction process, a better solution to electronic transactions the complex relationship of trust between the parties and secure connection, to ensure that electronic transactions in the authenticity, confidentiality, prevention of denial and can not be changed. But due to the large and complex of SET protocol, the banks, merchants and customers need to be modified to achieve interoperability; it still needs a process to widespread the use of SET protocol. In China, the most situations are that the application of the SSL protocol, there is still a long process to achieve the SET protocol.

2) Transaction security policy

a) Set up business and personal credit files.

b) To establish a signature credit system. In order to solve the problem of payer denied payment for the settlement, the bank should ask for the payer must be confirmed with payment and its signature. The commercial banks should keep the results of signature and payment records. Once the payment side denied the payments, the commercial banks can pay the order to produce the signature as evidence. To solve the problem of settlement funds into commercial banks to deny the recipient account, the recipient requires commercial banks to submit records of funds assigned to operate the digital signature. Recipient of the signature verification results is valid; it has been receiving recognition in order to continue to follow up with the payer’s business activities. Otherwise, the recipient refused to conduct follow-up.

c) Improve the laws of network security. Our government has stipulated in the “Contract Law of the People's Republic of China” that the electronic media as a carrier of the contract which has legally binding; and it has a great role in promoting the e-commerce. But in many aspects, it needs to adapt to the development of network technology constantly improve.

d) The government departments should focus on the existing form of virtual currency, the main body of issuance, standards the flow of virtual currency, to guide mainstream operators to regulate the gradual transition of third-party payment platform. And encourage the banks to develop innovative online payment service, in continuing to promote safe control technology based on the network, to meet the online banking services and facility needs of the consumer, and to maintain the fair of market.

3) The security policy for client

a) To raise the consumer's awareness of rational consumption and to establish a correct view of consumption.

b) To improve the personal awareness of online payment and to identify the fake website. To develop a unified software client application. The safety of the client on the impact of online payment security is one of the most crucial factors.

c) To enhance the security of the client, we can design and develop a unified payment terminal, unified standards. At the same time, the third-party payment platform can be incorporated into our financial management system, it is more reasonable in the market planning to increase security for online payment of the insurance factor. Meanwhile, it can bring convenience and security for the development of client software. It truly ensures the security from the very beginning.

IV. CONCLUSION

To sum up, the security is the most important factor for the third-party online payment platform. Due to it relates to the sustainable development of the third-party online payment platform. To ensure the security of online payment is not a thing accomplishes in an action, it is an ongoing task, it needs the continuous development and improvement. Our e-commerce is just onto the tracks, online payments grow very rapidly. To ensure the healthy and temperate development of the third-party online payment in our country, we must improve the management in various aspects. The each step in it should have a corresponding security policy, only in this way can the third-party online payment to achieve a substantial development in China, and it can achieve the strategies of sustainable development.

REFERENCES


