Mobile E-commerce Micro-payment Model and Its Security Technical Analysis

Weiwei Zhang

Nanchang Key Laboratory of material and structure detection Jiangxi University of Technology

Keywords: Mobile e-commerce; Mobile payment; Micro payment

Abstract. Based on the current situation of mobile e-commerce both at home and abroad, this paper indicates that as an important process of mobile e-commerce, the quality of mobile payment will directly affect the expansion of mobile e-commerce. Classified according to the business transactions amount, mobile payment can be divided into macro payment (more than $10) and micro payment (less than $10), for macro payment, security is a major issue, and the cost of it is quite high, so now most of the mobile payment is micro payment.

Introduction

With the rapid development of mobile e-commerce as well as the popularity of the Internet, more and more people join these, mobile e-commerce get love quickly because of its features of convenience and fastness, while mobile payment also becomes hot because of the drive of mobile e-commerce. The greatest feature of mobile e-commerce is that it is not subject to constraints of time and region, it can make people conduct their transactions anytime and anywhere, which also requires the mobile payment must meet this characteristic. According to the transaction amount, it can be divided into macro payment and micro payment, as the macro payment requires higher security technology, now people mostly choose micro payment. People's pace of life is increasingly fast, people also pursue fast-paced life, based on this, mobile e-commerce is also inevitably favored by people. Because of small transaction amount and convenient transaction of micro payment, there will be a broader platform for the development of the micro payment in the future.

Mobile e-commerce micro-payment model and its risk

Current development situation and trend of micro-payment model. In 1998, Nicholas • Negroponte of the MIT Media Lab had such prediction: "In the next few years, you will see the extraordinary action of using micro payment technology online", this technique will produce thousands of trillions of dollars of revenue each year.

Micro-payment gets more and more attention in the field of mobile payment, which became the main development direction of micro-payment and research hotspot of scholars. Currently, most of the mobile phone payment we usually use are within the scope of micro-payment. Such transactions are mainly for small amount of business between consumers and businesses, as the amount is small, requirements for security is not very high. Consumers can choose to pay by mobile phone rechargeable card or choose to bind mobile phone card with a bank card or a credit card, pay with a mobile e-wallet. For this kind of payment, consumers first have to fill the mobile phone rechargeable

card or bank card with a certain amount of pre-paid payment. Because of the popularity of mobile terminals, micro-payment has now become one of the research hot spots.

Target market of micro-payment model. Profit channels:

Mobile music:At present, mobile phone has been quite common, leading people to have a great degree of concern on digital music, the market scale grows rapidly, in Chinese digital music market, it gives first place to mobile digital music, including polyphonic ringtone, mobile phone ring tones, IVR mobile music on demand, etc.

Mobile email:The success of RIM company's black strawberry brought huge imagination to global wireless e-mail market, while the red strawberry business launched by China Unicom gives the infinite imagination to Chinese wireless e-mail.

Mobile search:The business myth created by the search engine in the Internet has attracted attention of many people, and mobile field is naturally the next Nuggets place of giants like Baidu and Google, 4G era is about to come, operators see more possibility of mobile value-added industry.

Target customers:

At present, people using micro-payment are mostly white-collar workers and college students, because these people are more receptive to new things and are willing to try and challenge, therefore, among users of micro payment, they are in the highest flight. Earlier, the Di Di taxi and Kuai Di taxi launched by WeChat, it is also them who first began to try, among them, college students are in the highest flight.

The target customers of micro payment are not limited to the young, there are still some middle-aged person, they have certain income, they are more relaxed than the white-collar workers, their mentality is relatively young, they like new things, so they are also willing to use micro-payment.

The risk of micro-payment model. Lost of mobile phone, PDA, laptop:

The main tool used for micro-payment are mobile phone, PDA, laptop, and you need to bind with the bank card password. However, if mobile phone or other tools are lost, then the account might be at risk. Because generally, bank card is bound with mobile phone or other, when the mobile phone is lost, the finder can select the "Forget Password" option, and then change the original password, so money in the bank card can be used by people who found it, this is extremely unsafe.

User information leakage:

It is almost a common problem, at present, most websites all have this problem, register an ID, then someone will send related information to you via QQ, some people are even accustomed to this, but it is really a considerable risk for micro-payment, as along as hackers get user's basic information, they can log in with user's information on their own mobile phone, PDA or laptop, at that time, user's money will be quite unsafe.

Account is stolen:

This is similar with the risk of losing mobile phone. After user registers an ID, there is

only one payment password, after the account is stolen, as long as the payment password is decoded, money in user's bank card is like in the hands of account stealer, he is free to use.

Security technology of micro-payment model

Security technology is the important guarantee for e-commerce transactions, in micro payment, because of the small transaction amount, it did not arouse too much attention, but because transaction volume is very large, the total transaction volume is very objective. Because the cost of a failed

transaction does not equal to the amount of that failed transaction, the main thing is that consumers and businesses lose trust, this intangible cost is enormous. Therefore this chapter performs corresponding research on micro payment by using the secure payment technology of e-commerce for reference.

Encryption. Encryption technology is a major security secrecy measures taken by e-commerce, it is the most common security secrecy measure, using technology method to change important data into messy code (encryption) and transmit, after the date reach destination, using the same or different method to reduction (decryption). The main purpose of encryption is to prevent unauthorized people to access information, it is the basis for the safe exchange among information via Intranet, Internet and Extranet, while encryption technology ensures the confidentiality of information, it can also ensure the integrity and correctness of information.

Symmetrical secret key:

Using encryption of one-key cryptography system, the same secret key can be used as the encryption and decryption of information, this kind of encryption is called symmetrical encryption, also known as one-key encryption. Because of its fast speed, symmetrical encryption is usually used when a message sender has to encrypt large amount of data. Symmetrical encryption is also known as secret key encryption. The so-called symmetry is that both-sides using method of this encryption method, using the same secret key for encryption and decryption. The secret key is the command for controlling encryption and decryption process. Algorithm is a set of rules stipulating the way for encryption and decryption. Thus, the encryption security depends not only on the encryption algorithm itself, security of secret key management is even more important.

Public secret key encryption:

Asymmetric cryptographic algorithm is also known as "public secret key encryption algorithm", the asymmetric cryptographic algorithm requires two secret keys: public key and private key. Public key and private key is a pair, if using a public key to encrypt data, only the corresponding private key can decrypt; if using a private key to encrypt the data, then only the corresponding public key can decrypt. Because encryption and decryption use two different secret keys, this algorithm is called asymmetric cryptographic algorithm. The confidentiality of asymmetric cryptographic algorithm is better, it eliminates the need for end-users to exchange secret keys.

Hash function:

Hash is generally translated to "hash", it also has a direct transliteration of "ha xi", that is, the input of any length (also called pre-image), through hash algorithm, converted into a fixed length output, which is the hash value. This conversion is a kind of compression mapping, that is, the space of hash value is usually much smaller than the input space, different inputs may hash to the same output, hash value can not solely determine input value. In brief, it is a function which compresses message of arbitrary length to a fixed length message digest.

Authentication technology. Authentication is also known as identification, it refers to a process that reliably verify whether the identity of payment participants is consistent with the identity he claimed, or whether a payment transaction is effective to ensure the authenticity of the data and prevent intruders to attack the system effectively. There are many means to achieve authentication, digital signature authentication, certificate authentication, etc. are common.

Digital signature authentication:

Digital signature (also known as public-key digital signature, electronic signature) is a kind of ordinary physical signature which seems like writings on paper, but using technology of public key

cryptography field to achieve, it is a method used for identify digital information. A set of digital signature usually defines two complementary operations, one for signature and the other for verification.

The so-called digital signature is some data appended on data unit, or password conversion done for data unit. This data or conversion allows data unit recipient to confirm the source and integrity of data unit and protect data to prevent people (such as receiver) from forgery.

The function of digital signature is to ensure the integrity of information transmission, sender identity authentication, to prevent the occurrence of transaction repudiation.

The digital signature is an encryption process, digital signature verification is a decryption process.

Certificate authentication:

Digital certificate is a bunch of digits marking the identity information of parties in the Internet communication, it provides a way to verify communication entity on the Internet, its role is similar to a driver's license or identity card in everyday life.

The simplest certificate contains a public key, name and digital signature of certificate authority center.

The principle is there are a lot of figures and English in digital certificate, when using digital certificate for identity authentication, it will randomly generates 128 bit identity code, each digital certificate can generate a corresponding but different digit each time, so ensure confidentiality of data transmission, which is equivalent to generate a complex password. Digital certificate bind a public key and the true identity of the holder, it is similar to identity cards in real life, the difference is that a digital certificate is no longer a paper license, but a section of electronic data containing certificate holder identity information and verified and issued by authentication center, it can be used more conveniently and flexibly e-commerce and e-government.

Characteristics of digital certificates are: safety, uniqueness, convenience.

Wireless application technology:

With the rapid development of Internet technology, a lot of information on the Internet is increasingly being introduced into the mobile phone, now just open the WAP mobile phone, no matter when and where, you can browse information and resource online, access wireless Internet. WAP services, such as news, weather forecast, games, pictures, music, etc., payment of these services are all micro-payment, it uses WAP global wireless application framework and network protocol standard, introducing the Internet and advanced data business to mobile phones and other wireless terminal devices by intelligence information transmission mode, WAP can run on a variety of wireless network to achieve compatibility and interoperability.

Conclusion

This paper compares the existing related materials of micro-payment at home and abroad, systematically explains micro-payment, including its definition, characteristics, safety technology and its risks. Finally, combining with WeChat payment, specifically explains advantages and disadvantages of micro-payment and safety analysis. Although there is some progress in the study of micro-payment of mobile e-commerce, but just under the current conditions, I believe that with the advent of 4G network and optimization of mobile environment, micro payment will develop more and more perfect. At present, China's various mobile operators have their own advantages, they have certain inherent advantages in terms of information acquisition, cost of infrastructure, market

development and the number of users. It can send and receive information anytime and anywhere, not subject to time and geography constraint, so that information can flow with the crowd.

Acknowledgment

This work was supported by Project on professional and characteristical construction of Jiangxi province 2010 (Civil Engineering) and Project on the planning and construction of disciplines in Jiangxi University of Technology (Structure Engineering)

References

[1] Ke Xinsheng Online payment and settlement[M] Beijing: Electronic Industry Press .2004.

[2] Liang Jin Core technology of e-commerce[M] Xi'an: Xi'an University of Electronic Science and Technology Press .2000.

[3] Huang Jing Micro-payment study in mobile e-commerce [D] Hubei: Central China Normal University, master's degree thesis .2006.

[4] Xiong Xiaofang, Yang Yitao, Li Yan, etc. Research on mobile e-commerce micro-payment model [J] Nanchang Junior College, 2006,65 (4): 33-38.

[5] Li Dongyun Research of secure payment technology of mobile e-commerce [D] Hunan: Central South University, master's degree thesis .2002.

[6] Lu Lin Research on digital signature and micro-payment protocol of mobile e-commerce[D] Chongqing: Chongqing University of Posts, master's degree thesis .2013.

[7] Sun Xun Research on security certification and payment protocol in mobile e-commerce[D] Chongqing: Chongqing University of Posts, master's degree thesis .2010.

[8] Feng Dengguo, Pei Dingti. Cryptography Guide[M] Beijing: Science Press. 1999.

[9] Bruce Schneier, Wu Shizhong translate, Applied Cryptography: Protocols, Algorithms and C source program[M] Beijing: Beijing Machinery Industry Press .2000.

[10] Lehman Brothers .Moving in mobile media Mode[J].Journal of American Science,1995.

[11] Fung Jack .Mobile Portal Supportive System Suggestion[J] .Motorola GTSS.2002.