Research on Internet Payment Security Based on the Strong Authentication of the Timeliness and Multi-factors

Junsheng Wang[1, a], Qingsu He[2, b] and Qingzhi Han[1, c*]

[1]Beijing Huitong Financial Information Technology co.ltd, Beijing 100032, China

[2]Internet Financial Laboratory, Beijing 100032, China

[a]heqingsu@sgitg.sgcc.com.cn, [b]19158382@qq.com, [c]hqz1245086050@126.comil

*The corresponding author

Keywords: Security and convenience; Internet payment; Timeliness; Multi-factors and strong authentication; Payment efficiency

Abstract. Security and convenience is the main consideration for the user to select the Internet payment, and also the key issue of the development of the Internet payment industry. At present, on Third-Party Payment Platform, E-bank and other Internet payment platform, when users change the password, pay or transfer account, only phone verification codes or password are given to complete the transaction, but it is extremely trouble to ensure the safety of people's funds. To solve this problem, a secure and convenient payment mode based on the Strong Authentication of the Timeliness and Multi-factors is proposed in the paper. When registered the payment account on the internet, users need have at least two authentication methods that are randomly select from the methods given by Internet Payment Platform and input their information for payment verification. When users login the Internet Payment Platform for the first time, every authentication method that users select must be input and the information be correct as well. After that, within a specified time, each payment is reduced by one authentication factor, but ultimately not less than a pay factor.

Introduction

The Internet Finance has been a continuing concern in recent years. With the rapid development of Internet information technologies such as social networks, mega data and cloud computing, Third-Party payment, P2P, Internet loans and financial institutions online platform as the representatives of Internet Financial Model has formed. Internet payment has become an indispensable part of Internet Finance, so we should pay more attention to its safety [1, 2, 3, 4, 5].

Currently, the users in the Internet to pay the transaction only need the password or phone verification codes, however, the authentication method of “the user name + password” is easy to be embezzled or tampered with [4]. The authentication method of "password + phone verification codes" is that when users login the Internet Payment platform, which will generate one-time verification codes to send to users' Phone numbers bound at the time of registering account; Although this method is more secure than a single static password authentication, but today, as a variety of telecom fraud means, phone verification codes are obtained by illegal ways as easy as pie, for example renew SIM/STK card by online business provided by mobile operators. Therefore, the authentication method of "Password + phone verification codes" is also very unsafe [5].

Due to the rapid development of Internet technology and biological technology, in order to improve the security of Internet payment, some Biometric Identification Technology contained features of the unique and impossible to be copied and never lost have been applied to Internet payment [6, 7, 8]. Password has been no longer the only authentication payment method, so we consider the combination of different kinds of certified payment methods to complete Internet payment transactions, which can ensure sufficiently the financial security of users, even if the users' password, mobile phone and other personal information are missing or leaked.

Based on the above analysis, a secure and convenient payment mode based on the Strong Authentication of the Timeliness and Multi-factors is proposed in the paper to guarantee the security of the users' Internet transactions with a positive experience.

Security Issues of Internet Payment

Internet payment in the convenience of users shopping and servicing aspects of the development of electronic commerce has played a significant role. But at the same time, fraud means is innovating constantly, users are lack of cognition of Internet payment risk, and the authentication method of Internet payment platform exists greatly defect, which results in the transfer of many users' finances illegally through Internet payment channels. At present, the security issues about Internet payment mainly are as following.

Fist, security problem of inputting simply password to complete payment

Users' payment account and password is stole by the phone virus or phishing sites. Once the mobile phone is implanted Trojan, the user message, mobile banking account, Alipay account and other personal privacy information can be purloined by lawbreakers, and then the Digital Certificate and other safe settings are canceled. Then lawbreakers transfer all types of messages to the specific cell-phone number and shield the payment confirmation SMS. Ultimately, cell phone payment verification codes are embezzled, and break the user's payment account number and password [9]. Or the criminals send false information by an SMS or e-mail to induce users to enter a false websites with conditions similar to those on the real Internet payment platform. Then the account and password which users input are recorded by the backstage database, thus causing great loss of properties to users in a short period.

Second, there is security issue when Third-Party Payment Platform binds bank card.

When blinding account number on Third-party Payment platform to enjoy the function of Quick Payment, users only need to input bank card number, which easily is token advantage of by criminals to transfer customers' finance, once lawbreakers obtain the users' ID card, bank card number and other personal information.

Third, security hole using phone verification codes to changed account and password.

The messages about abolishing mobile value-added services are sent to consumer to cheat the users of phone verification codes, leading to the replacing of the phone number's owner. First of all, criminals decode the password of web portal of mobile operators to change the owners' phone card. When users login page to start the process of changing the phone card, one-time verification code generated by the site system is sent to users' mobile phone. Then criminals send the messages about abolishing mobile value-added service to users for getting their phone verification codes, which is the foremost step to replace the phone numbers' owner. Eventually, criminals can effortlessly login and tamper with the Internet Finance accounts of users, for example Aliped, Baidu Wallet ,E-bank, so that founds bound the Internet Finance Platform and the bank cards are transferred to the criminals' accounts. That is to say, if users' phone verification codes are plundered, a series of safety verification of Third-Party Payment Platform and bank will be no longer in force, ultimately, which causes that all funds of users are ransacked.

So, phone verification codes can be used to rewrite various information of the Internet Finance account such as changing the account and password, which enables the two-factor authentication to become the one-factor authentication, resulting in the decline of security drastically.

The Security Mode Based on Multi-factors and Strong Authentication

With the continuous renovation of the Internet fraud means, the risk of the payment method of password become increasingly prominent; especially mobile Internet payment provides customers with high efficiency, bringing also many great risks of payment. Although the technology of Internet payment authentication is still innovating constantly, and biometric technology is applied to the Internet payment, which can enhance the security of payment to a certain extent, it is difficult to insure the payment security only relying on a kind of payment authentication tactics, from the second section of this paper as well as in the long run [10].

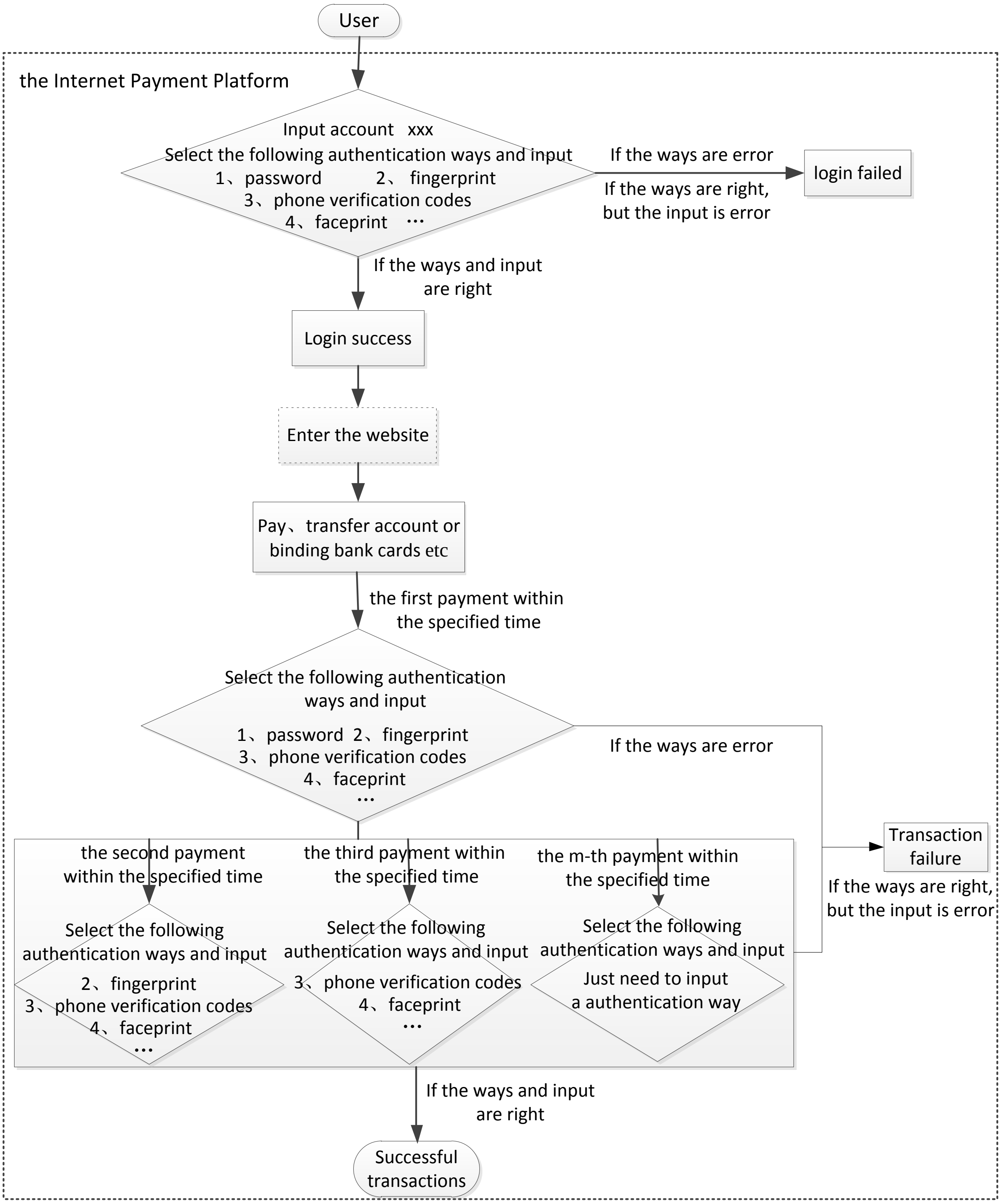
User
the Internet Payment Platform
Input account xxx
Select the following authentication ways and input
1、password 2、fingerprint
3、phone verification codes
4、faceprint …
If the ways are error
login failed
If the ways are right, but the input is error
If the ways and input are right
Login success
Enter the website
Pay、transfer account or binding bank cards etc
the first payment within the specified time
Select the following authentication ways and input
1、password 2、fingerprint
3、phone verification codes
4、faceprint
…
If the ways are error
Transaction failure
If the ways are right, but the input is error
the second payment within the specified time
Select the following authentication ways and input
2、fingerprint
3、phone verification codes
4、faceprint
…
the third payment within the specified time
Select the following authentication ways and input
3、phone verification codes
4、faceprint
…
the m-th payment within the specified time
Select the following authentication ways and input
Just need to input a authentication way
If the ways and input are right
Successful transactions

Figure 1. The payment mode based on the Strong Authentication of the Timeliness and Multi-factors

In this paper, considered the security and reflected the characteristics of the convenience and quickness of Internet payment, a payment mode based on the Strong Authentication of the Timeliness and Multi-factors is proposed. In this mode, different authentication factors about Internet Payment are added to ensure the accuracy of the identity information of the users. In this mode, different authentication factors about Internet Payment are added to ensure the accuracy of the identity information of the users. At the same time, considering that users may feel a lot of trouble when carrying out multiple payment operations, the certification factors should be paid on the basis of its timeliness.

First of all, when users register Internet Payment account, in addition to verifying the user's identity information, the different authentication methods for login and payment must also be reserved and inputted to establish the identity of users. And the Internet Payment Platform must provide users with many different authentication methods that contained in users reservation, for example passwords, fingerprints, palm prints, sound, iris, etc, and users randomly selected at least three from them for payment confirmation.

Then, when users complete the registration and login the online payment platform to pay, to transfer account, to bind bank cards for quick payment on Third-party Payment Platform or some other dealings, the reserved payment authentication methods must be selected and inputted.

Finally, only all of information selected and inputted is accurate, the online transactions can be successful. Otherwise, any kind of authentication method chosen or inputted is wrong, the transaction fails. As shown in Fig. 1.

Summary

The unification of security and convenience about Internet Payment is the core of development and prosperity of Internet Financial. Convenience is the outstanding advantage of Internet payments over other payments, and payment security is the essential guarantee for the sustained and healthy development of Internet Financial. Internet Payment without a certain degree of security will not be received by the majority of users, and there will also be no payment demand. The Internet Payment model proposed in this paper can provide users with the maximum degree of convenience on the basis of guaranteeing the security, strive to achieve the balance of the payment security and efficiency, improve the existing Internet Payment environment, and promote the development and prosperity of the Internet Payment industry.

Acknowledgements

In this paper, the research was sponsored by the Science and technology project of state Power Grid Corp (Project No. 9900/2017-6314B).

References

[1] KIM C S, GALLIERS R D, SHIN N, et al. Factors influencing Internet shopping value and customer repurchase intention, J. Electronic Commerce Research and Applications, 2012, 11(4):374-387.

[2] E.L Li. Assessment of Third-party Payment Security Using Attack Tree, J. Application Research of Computers, 2014, 31 (4):1204-1208. (In Chinese)

[3] J. Yao. Research and Countermeasures on the Security Problem of Third - party Payment in E-commerce, J. Finance and Economy, 2014(11). (In Chinese)

[4] Information on http://finance.sina.com.cn/money/roll/20151020/135823524553.shtml

[5] Information on http://finance.ifeng.com/a/20151014/14018320_0.shtml

[6] H.Z. Li, G.G. HAN and Y. Wang. Provable Security Research on User Authentication Scheme of Roaming Network, J. Netinfo Security, 2015(7):51-57. (In Chinese)

[7] Y. Fan, J. Xu and Y.T. Gao. Research and Implementation of eID-Based Identity Authentication System, J. Netinfo Security, 2015(3): 48-53. (In Chinese)

[8] SOOD S K, SARJE A K, SINGH K. A Secure Dynamic Identity Based Authentication Protocol for Multi-server Architecture, J. Journal of Network and Computer Applications, 2011, 34 (2):609-618.

[9] LEE C, LIN T, CHANG R. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment Using Smart Cards, J. Expert Systems with Applications, 2011, 38 (11):13863-13870.

[10] J. Xu, Y.N. Zhao, Y.C Tian and F.C. Zhou. Research on Conference Identity Authentication System Based on Two-dimensional Bar Code and Face Recognition, J. Netinfo Security, 2015(4):13-18. (In Chinese)

[11] Y.Q Zhang, Z.Q. WANG, Q.X Liu, J.P Lou and D. Yao. Research Progress and Trends on the Security of Near Field Communication, J. Chinese Journal of Computers, 2016, 39(6):1190-1207. (In Chinese)

[12] Q.Y Ge and L.J Che. Research on Multi-factor Authentication Mode for Online Security Payment, J. Netinfo Security, 2015(12):48-53. (In Chinese)