ATLANTIS PRESS
Advances in Computer Science Research, volume 71
4th International Conference on Machinery, Materials and Information Technology Applications (ICMMITA 2016)

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

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

[1]BEIJING HUITONG FINANCIAL INFORMATION TECHNOLOGY CO.LTD, Beijing 100032, China;

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

Keywords: Internet payment; Security risk; Phone verification code; Multi-factors and Strong authentication.

Abstract. Internet payment with the rapid development has brought great convenience to people's lives, but also tremendous security risks people's property. At present, on Third-Party Payment Platform, E-bank and other Internet payment methods, to change the password, to pay or to transfer account, only phone verification codes or password are given to complete the transaction; When disclosure of personal information such as phone and password is stolen, or user access to phishing sites, it is extremely trouble to ensure the safety of people's funds. The method of multi-factors and strong authentication is proposed in the paper for the security problem about Internet payment. When the user is Internet payment operations, the phone verification codes provided by the mobile operators are not unique authentication system, but also the need for the payment authentication system to be set aside for the Internet payment account.

1. 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].

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. Through the analysis of the above problems, an Internet security payment model based on multi-factors and strong authentication is proposed in this paper to guarantee the security of the users' Internet payment transactions.

2. 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 Alipay, 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.

"Accounts automatically buy financial products" to cheat the users of phone verification codes. Above all, the users' E-bank account and password are stolen through illegal means by criminals, for example, by sending SMS Trojan link, and secretly "help" users to purchase financial products and be bound on the Third-party Payment platform, which leads to the drastic reducing of the users' funds. Fortunately, at the moment, the funds still beyond to the users. Then, criminals create an atmosphere of tension, and a string of numbers (the numbers are essentially the phone verification codes sent by the bank) by the messages about cancelling the purchase of financial products are sent to users. Finally, after users tell the criminals the codes, they will transfer users' funds to the bank accounts held by criminals.

As will be readily seen, 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.

3. 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].

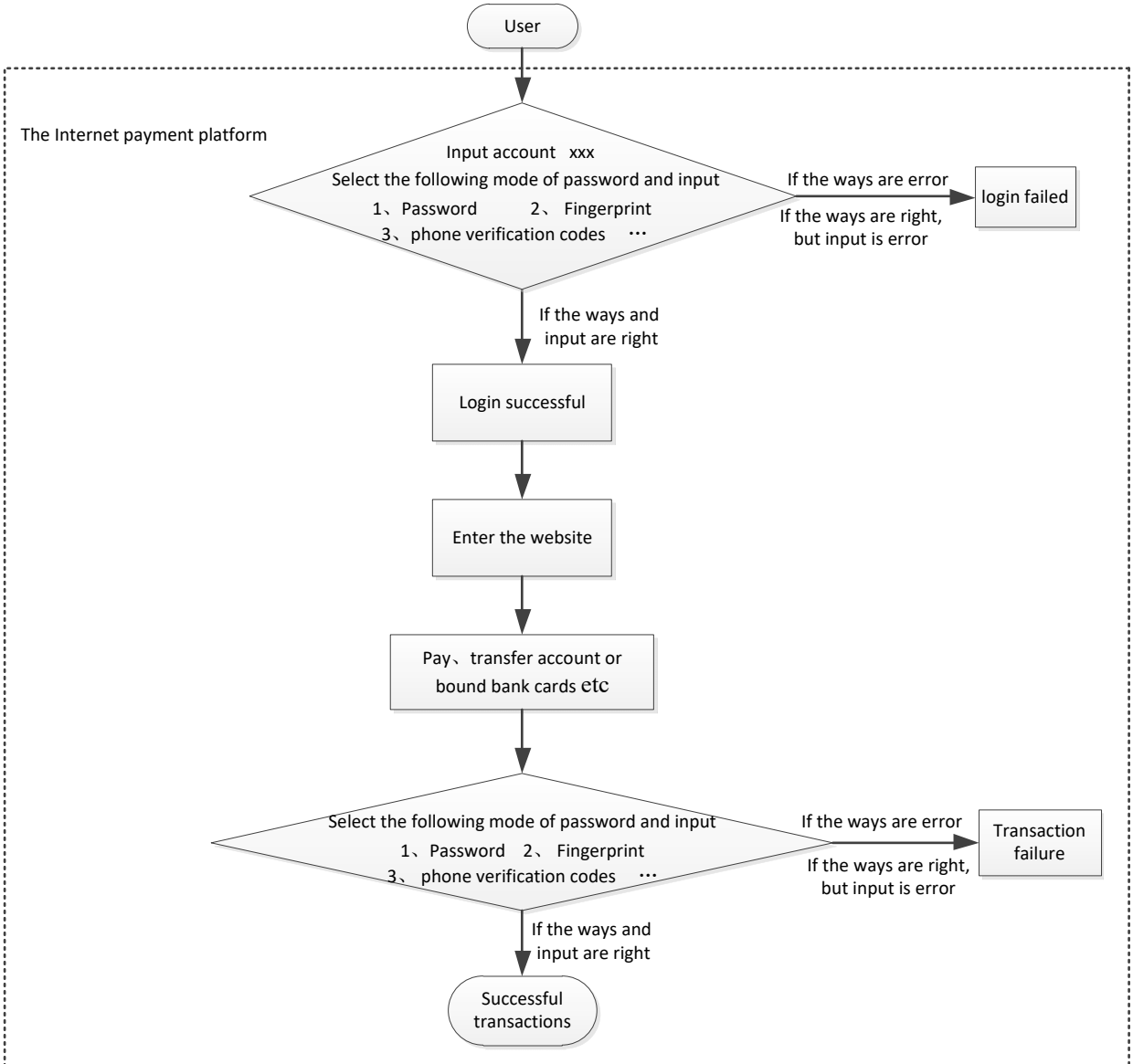

Fig. 1 The security mode based on multi-factors and strong authentication

In order to ensure the accuracy of user' identity and the security of payment, the mode of Internet payment based on multi-factors and strong authentication is proposed in the paper. First of all, when users apply for e-bank accounts in bank branches, a variety of payment authentication methods, for example passwords, fingerprints, palm prints, sound, iris, etc, must be provided for users to choose, and users randomly selected one or several from them for payment transactions. Then, when users complete the registration and login the online bank to pay, to transfer account or some other operations, the web portals must have also a variety of options of payment authentication ways for user. Finally, only when the payment authentication methods users select are accord with that reserved in bank branches, and the information inputted should be correct as well, the payment can be completed. Similarly, when users use Third-party payment platform for quick payment to bind bank

cards binding, it also need to have the same mode of payment with that of online banking. As shown in Figure. 1.

4. Summary

Internet payment security is the essential guarantee for the sustainable and healthy progress of The Internet Finance. Although the distinct advantages which the Internet payment, especially mobile payment, compares with other payment methods are convenience and efficiency and good user experience, if there is no security, it will not be received by the majority of users. To a certain extent, convenience and efficiency are at the expense of security. Notwithstanding, the payment way proposed in this paper will have some complexity when users operate on Internet payment platform, it can ensure high enough security. And only settling the problem of payment security, network payment industry can develop prosperously and continuously.

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.

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

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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