Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):437-441

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Research of network payment system based on multi-factor authentication

Jiang Yuyan and Li Changxun

School of Management Science and Engineering, Anhui University of Technology, Ma'anshan, China

---

ABSTRACT

With the increasing popularity of e-commerce, its safety performance have also been extensive attention, along with a need for a safe and efficient authentication system. This paper analyzes the main currently used authentication method, According to the defects present a combination of USB Key, static password and the new dynamic password authentication method of payment systems, which have greatly improved the security of online payment.

Key words: USB Key; dynamic password; authentication

INTRODUCTION

With computers, networks and information technology development and increasing integration, Internet has entered people's social life in all fields and links. However, in the most central and most important of e-commerce is e-payment link. Digicash, First Virtual, Netbill, SSL, SET is e-commerce transactions agreement , but only the SSL and SET[1] is the most commonly used. SET protocol and SSL protocol are recognized industry standard protocols, the establishment of the electronic payment platform based on these two protocols is more reliable and safe. The related products around these two agreements have been more mature .

For the SSL protocol, the SSL protocol embedded in the realization of it on Microsoft and Netscape's browsers. With the SET protocol, RSA, IBM, VISA companies have the related products[2]. Domestic e-commerce research is relatively backward, there is no mature form their own related products, however, security products research is the issue of national interest, for the security products we can not rely on imports, therefore, based on the need of our own development of domestic e-commerce to study the safe, reliable and convenient electronic payment system is very important.

Currently, the key to online payment authentication is the following three ways or a combination of these[3]:
1, the user knows a secret information such as user passwords

2, a secret information held by the user (hardware), the user must hold a valid physical media such as magnetic cards, smart cards, USB key or the user public key certificate.

3, the user has certain biological characteristics, such as fingerprints, voice, DNA patterns, retinal scans. A way of using one of them is the single-factor authentication methods, combined with a variety of ways is the multi-factor authentication. Single-factor authentication in any of these factors are likely to be guessed, stolen or attack, and multi-factor authentication is a strong authentication method, it is more than an ordinary single-factor authentication technology with higher security. This paper proposed a combination of a static password, USB key and SMS dynamic password authentication system, to achieve a two-way authentication system, and greatly improves network security in the payment process.

USB KEY TECHNOLOGY

USB KEY-based authentication method is developed in recent years of a convenient, secure, reliable authentication

techniques. It is easy to carry, easy to use, low cost, coupled with the complete data protection mechanisms of PKI system, so that it is recognized as the most secure online identity by the related user, was used throughout all aspects of electronic trading . Digital certificate is issued by Certificate Authority (CA) that contains a set of user identity information (keys), public information data structure, and authoritative third-party CA's digital signature, which can ensure the integrity of information transmission and digital information can not be repudiation. PKI system through the use of encryption algorithm to construct a comprehensive process to ensure that the digital certificate holder's identity and security. USBKEY can protect the use of digital certificates can not be copied, all the key to be achieved in USBKEY , the key is not in the computer memory and does not appear in the network, only USBKEY holding people to operate the digital certificate, security has been protected.

USB Key authentication system is mainly related to the user, the bank WWW server, bank server, CA center server and the USB Key five parts, the operation shown in Figure 1.

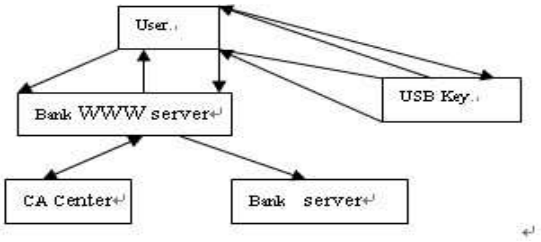

Figure 1: USB Key authentication system

1.Users Login banking sites
2.Prompted to insert the USB Key, and enter the PIN code
3.Users enter a PIN code
4.Prompted to verify through
5.Import exchange needed data
6.Data with a private key to sign, encrypt
7.User certificate, the signature data to the bank WWW server to verify
8.CA Center server for the transmission user certificate and the signature verification data to determine the user identity
9.Bank WWW server using the public key in the user certificate to verify the encryption information and the transfer and other operations after it is verified.

While the USB Key authentication technology with high security ,however, even if it is verified but not fundamentally guarantee " the person using the USB Key is indeed the person authorized to use the USB Key." Because the PIN is input through the computer, hackers can get the user's PIN code through the process, if the user does not promptly removed USB Key, hackers can received a false certification by intercepting the PIN code, damage the interests of users, so only use the PIN layer of protection does not ensure security of users use the USB Key.

OTP (DYNAMIC PASSWORD) TECHNOLOGY

Traditional authentication technology is mainly static password authentication, but the leak and static nature of it's own shortcomings can not put enough sufficient access security. In 1981, the first proposed one-time password generated using the hash function by the American scientist Leslie Lamport, that each time a user to connect with the server process, use the Internet password is encrypted cipher-text when transmitted, and cipher-text in these each connection is different, that password is a valid cipher-text. OTP technology with continuous development and improvement. Dynamic password currently used methods of payment: password card, mobile phone software tokens, SMS, password card. In the process of using these methods, we found that mobile software tokens has the problem of compatibility ,passwords card is easily to lost and other issues .These problems lead directly to br obstructed in the universal process.

At present, some sites during the authentication process using the browser verification code, it is usually randomly generated by the server, usually by a string of numbers and letters, showing the landing page. When the user logs must be input verification code and submit, validate the submited verification code on the server that hackers can not use a dictionary attack. However, the security problems of inputing verification code on browser still exist [4]: If the verification code in text form to the client, hackers use monitoring tool, they can intercept the verification code in the transfer, the role of security failure. If the verification code to make image format, because the image is to use binary transfer, verification code is very difficult to direct read, it can enhance the verification code security and defense

capabilities. But the attacker still can use image-recognition technology, such as OCR software recognizes the characters on the picture, the picture characters revert to text characters. Adding noise to increase the difficulty of picture identification to prevent, there may seriously affect the user's convenience. However, do take credit card online banking process, will be asked to fill out one's cell phone number, bank card and cell phone will be binding, if every time the dynamic password will be paid in the form of text messages sent to the bound phone, hackers can not use the software to steal user's mobile phone information, the payment can be efficient to ensure security.

THE CERTIFICATION PROGRAM DESIGN

Based on the above analysis, this paper present an improved authentication system of combining USB key and the message dynamic password, this authentication system in the original text to add a dynamic password authentication part, for the gift to a system's security layer of defense to better overcome a number of inherent defects of the USB Key authentication system, it is safe, efficient, easy, etc., very suitable for the authentication part of the payment system with the current network environment.

User application to the CA certificate, the users' application information, such as name, e-mail, ID number, phone number, etc. (M + KUSRpub)will start the application process reached the system's encryption program. The right data will be transfered to the cryptographic service provider (CSP) program by the encryption program. On the user's computer will generate a public key and a private key, two keys are usually referred to as key pair. After key generation, CSP will encrypt and protect security of private key, the private key will be stored in the USB Key in the individual. Public key together with the certificate applicant information is sent to the certification authority CA. If the CA mechanism based on its strategy to confirm the certificate request, it will use its own private key to create a digital signature on the certificate, then the certificate (M + S + KCApub + KUSRpub) issued to the applicant.

Subsequently, the applicant will receive a certificate from the CA certificate installed in the appropriate computer. The data included in the certificate from the certificate subject's public key and encryption key for the public. For the sender's private key to sign with the message, the message recipient can verify the sender's public key authenticity. The key can be find a sender's certificate. Using the public key certificate to verify the signature, can confirm whether the signature is generated using the private key of the certificate subject. If the sender has been good to maintain the confidentiality of the private key, the receiver can be confident that the message sender's identity. The concrete operational stage of the payment process is as figure 2:

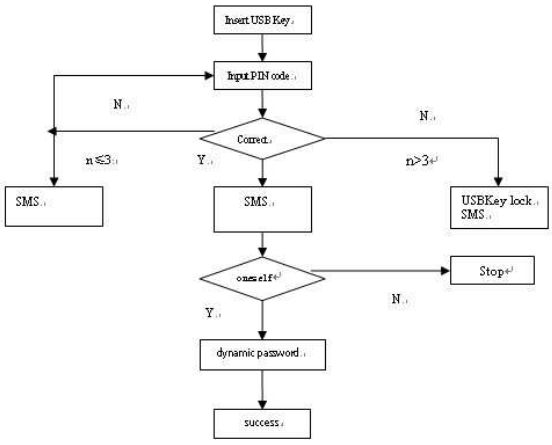

Figure 2: certification system operating process

System operation process is as follows: for payment, the system prompts the user to insert the USB Key to submit the certificate (M + S + KCApub +KUSRpub), the server with the CA's KCApub signature to verify the information on the H / = KCApub (S), verify the results compared with the original summary H = hash (M), if H / ≠ H, the signature is error, the system refused to sign; if H / = H then the signature is correct and the certificate may continue to operate, as shown in Figure 3 [5].

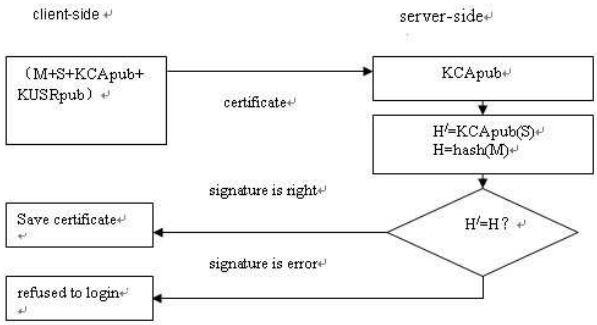

Figure 3: certificate validation process

After the server to verify the certificate, the certificate holder is also verified, as shown in Figure 4 [5].

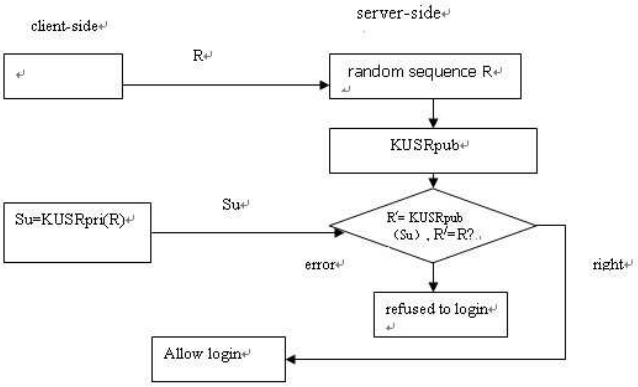

Figure 4: certificate holder validation process

After verifying the certificate holder is a legitimate user, the user input a PIN code what has been set according to requirements, if the enter PINcode is different with the real user set in banks, the wrong is less than three times refused to register, and SMS notification that someone is using their online banking password wrong to the real users; if three or more wrong, USB Key automatically lock and text messages to inform. Because the PIN is input through the computer, hackers can get the user's PIN code through the process, so even if the PIN is verified not fundamentally guarantee " the person using the USB Key is indeed the person authorized to use the USB Key." On this basis, it is necessary to further the identity of the user authentication, the server dynamically generates a random password and send a text message to a cell phone has been bound, subject the user himself, the dynamic password is entered correctly operate smoothly; If someone using is not the user, not within a certain time dynamic password is entered correctly, the operation terminates.

SAFETY ANALYSIS

network: eavesdropping. General USB Key authentication system usually only take the dual protection of USB Key hardware and PIN, because the PIN is transmitted in the network so easily hacked and stolen, and the use of hardware devices are not removed in time for illegal operations . The improved authentication system based on the original message with a dynamic password authentication part, due to the dynamic password is not directly transmitted in the network, an attacker can not eavesdrop on the user's password, which effectively protect against network eavesdropping attacks.

the interception / replay attacks: Because of the uncertainty factor to generate dynamic password is constantly changing, such as S / KEY password authentication, each time authentication is successful, the user authentication server will automatically reduce the iteration value 1,which makes the next time a user logs calculated data is different with the previous answer, the user receives a text message every time and submit to the network authentication password is different, so as to effectively resist the replay attack.

counterfeit server: The improved system implement a two-way of user and server authentication, the server can better withstand the risk of forgery.

password guessing: The multi-factor authentication system, not only relied the passwords what can be guessed for security protection, in addition, also the use of uncertainty factors to generate dynamic password, even if the PIN has

been stolen can effectively protect the safety of users.

We can see that the authentication system can effectively resist the most of network attacks, the security has been significantly improved, in particular, can be effective against network eavesdropping, interception / replay, password disclosure, social engineering and other forms of attack.

REFERENCES

[1] Cao Haiping， *Application of computer system*, **2006**(6):58-60
[2] Xiao Shi-cheng Li Kai Gan Zao-bin, *Computer science*，**2012**,39(3):75-78
[3] Zhong-Xian Li Hua Zhan， *Electronics Technology*，**1999**,27 (1): 98-102
[4] Deng Jing, OTP-based technology, online banking security authentication application of [D]. Foreign Trade and Economic University,**2006**.4.1
[5] Zhang Yihui, Wang Zhaoshun. *Aviation Computing*, **2007** (4)：129-131