Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A COMPREHENSIVE ANALYSIS OF ATTACKS ON ONLINE PAYMENT SCHEMES

[1] LINA ZHANG, [2] WENBIN YAN

[1]Department of Computing Science and Technology, Xi'an University of Science and Technology, Xi'an 710054, Shaanxi, China

[2]Department of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

ABSTRACT

When payments are to be made over the Internet, security becomes critical. The online banking system has become the preferred target of some attackers. To maintain the clients' trust and confidence in the security of the services, the financial institutions and related research workers must identify how the attackers damage the user's account and develop methods to enhance the security of the system. Based on analyzing the basic processes of online payment and the mode of attacks, the security and general prevention techniques are discussed. A complete analysis of the attack process in the transactions is given. In addition, some secure schemes and corresponding system design strategies against aggressive behaviors are proposed. This analysis and schemes are intended to be useful for commercial banks to adopt or to improve their online banking systems.

Keywords: *Online Banking, Public Key Infrastructure, Cryptographic Service Provider, Smart Card, Signature*

1. INTRODUCTION

Internet technology has influenced almost everyone's life during the past few decades. Commercial banks set up workstation by the internet and provide customers information requirement, financial services of internet payment、fund diversion, Credit, investment, etc. The development and popularization of online banking [1] have brought efficient life to people in recent years and it has spread rapidly in all countries of the world as a result of its convenience and ease. Spurred by rapid growth of the usage, a number of the studies about online banking have been performed around the world. However, the research has mostly been focused on the issues of the accessibility and compatibility of online banking, the customer satisfaction, the customer attitude towards online banking usage [2, 3] and the improvement of concrete cryptographic algorithms [4].

As the number of clients increases, online banking systems are becoming more desirable targets for attackers. A lot of issues, such as the users' bank account number and password were stolen and illegal transfer of account funds has brought huge losses to banks and individuals [5]. Security has become one of the important factors for e-commerce application and user to choose which online banking for their payment. Now the transaction security has become the bottleneck of the further development of online banking and we need to shift the focus of research about it.

To maintain the clients' trust and confidence in the security of the services, the financial institutions must identify how the attackers damage the user's count and develop methods to enhance the security of the system. Online banking system's security issues involves in a number of aspects, including the security of the server system, the trading communications, the encryption algorithm, and the operating security of the users, etc. This study focused on analyzing the basic transaction processes and its security and discusses the security and prevention techniques. It assumed that an attacker could use various means to attack a client's computer. Through the model this study gave, the user's trading could also be controlled within a range of security even that the computer was completely controlled.

2. RELATED BACKGROUND OF THE PAYMENT SYSTEM IN ONLINE BANKING

Internet banking is also known as "3A Bank." It is not subject to the restrictions of time and space, at any time (Anytime), anywhere (Anywhere) in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

any way (Anyway), to provide customers with convenient financial services. These services are based on the Internet which is open to everybody，thus it gives users a new way of life, while also making them facing the ever-increasing range of attacks and fraud. They have taken the appropriate security mechanisms [6] to ensure the security of online banking. It needs to ensure the confidential information such as the user name, bank accounts, login pin, transaction password and data not to be leak or theft. In the design of the system, it uses cryptography mechanism that encryption mechanisms [7, 8] to ensure the data confidentiality, digital signature mechanisms [9] to ensure the integrity and non-repudiation of the data, digital certificates [10] to store the user's public / private key in general.

2.1 Cryptology Technology

Cryptography and cryptanalysis are two aspects of cryptology techniques. Cryptography is the study on crypto system design and knowledge to hide information through encoding; cryptanalysis is the study of how to decipher the encrypted information or information forged. Cryptography and information technology have become a significant foundation for information security. Encryption / decryption and digital signature technology is prominent contents of cryptography [11].

Data information would be very vulnerable to eavesdropping, interception, tampering and other attacks in the process of interaction and transmission in the form of plaintext. The encryption technology is an effective means to protect the confidentiality of the data; the digital signature technology is mainly used for authentication and non-repudiation of the signature information. Usually, in order to ensure the safety of the communication data, the interaction data need to be encrypted and encapsulation, and then transmitted through a secure channel. It also needs to add a digital signature with the data to ensure the authenticity of the identity, so that the receiver can confirm that the message was sent by a trusted party.

2.2 PKI And Digital Certificate

Public key infrastructure (PKI) system is used extensively at present to solve the security of Network Information Services. It is a certificate and key management system, which provides cipher service for all kinds of network application, such as encrypt and digital signature. It provides an extensible and policy-based method to solve identification and non-reputation.

CA (Certificate Authority) is an authentic third organization in PKI, which offers authority, creditability and notarization to all the registered users. CA issues' digital certificates are to validate electro-entities in the net and manage the certificates.

PKI is one of the key security technologies on the Internet, and it is a base to provide Internet security services using the public key certificates. Currently, more and more security policies based on PKI are used in online banking.

2.3 Cryptographic Service Provider

Microsoft Windows' OS provides users with all application program interfaces for cryptography by Cryptographic Service Provider (CSP) [12]. Application developers can use the functions in Crypto API, which works with a number of CSP without knowing details of the underlying implementation, in much the same way as they can use a graphics library without knowing anything about the particular graphics hardware configuration.

As smart card has been becoming the mainstream of data-storage materials, the encrypt server based on CSP could provide higher security by combined with smart card. CSP could only afford RSA, DSA, DH [13], and many symmetric algorithms such as DES and RC4.

Currently, the application based on CSP is mainly in PKI construction, identification, access control systems. It could achieve good transplant with the ability of device-independent encryption function and be used with the certificate system through PKCS interface. As a generic specification, it has gradually become the industry standard, and a growing number of encryption equipment manufacturers is developing products with the standard interface of CSP.

3. ATTACKS AND SECURITY ANALYSIS IN THE PAYMENT SYSTEM

The most important security issues [1] in the online banking payment system can be summarized as a confirmation of the user identity and communication information. It is simple to use the username + password to login in when authentication is required and ordinary mechanisms to ensure the integrity of the transaction information in the early stages. These easy safety measures led to a large number of users' accounts to be stolen and invaded [14]. Online banking used various types of cryptography security mechanisms in this respect. The soft keyboard must be used to enter the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

password, and the client is forced to install anti-Trojan software that could scan the keyboard driver to prevent the Trojans and so on [15-17]. These technologies in certain extent protected the security. However, with the increase in defense modes, means of attack is also escalating.

Three types of system attacks and prevention techniques are summarized in Table I and descript in details in the following three sections.

TABLE I: Attack Ways Of Online Banking

Means of attacks	Target	Technology
Phishing	Get the use's password	XSS attacks, junk mail, URL simulation, page simulation
Keyboard record	Get the use's password and transaction pin	Key hook, message hook, to hijack the keyboard interrupt, remapping in the IOAPI table
Tamper with signature data and the trading pages	Forge the trading	Inject the DLL to the IE browser

The first type is the false URL access deception.

When accessing to online banking, the users were vulnerable to be deceived as "phishing" attacks. Aggressive behavior usually occurred when the client used a WEB browser to enter an address or clicked on a page address link to access online banking. The attacks typically use a variety of means, such as spam attacks, cross-site scripting (XSS attacks) to induce the user to click on phishing URL address of the real site to get the user's bank or credit card account numbers, passwords, and other important information.

Such attacks are very simple, such as advertising, false winning information to achieve by sending large amounts of junk mail. The technology and implementation cost is very low in this attack, so this is also the place where most of the security problems occur of online banking. With this attack, the attacker can get a large number of the user's login name and password, to that the large numbers of the user's personal information are compromised.

A simple measure is to set the black or white lists in the client to prevent the user accessing to illegal URL. Now online banking in general is to force the user to set different values with the login and transaction pin, and ask users to reserve verification information when access in the first time. If logging in phishing sites, the user inevitably couldn't see the verification information. Then the user can immediately log on legitimate sites to change his password, or call the bank temporarily blocked the account.

The second type is record keyboard input.

The typical login mechanism of online banking only requires the user to enter the name and password through the keyboard. The system model and attack methods are shown in figure 1. The attacker can easily obtain user's key information by keyboard recording programs, and the aggressive behaviors occurred when the client filled in the user name and password to login on the online banking. The specific methods of attacks are using keyboard hook, log hook, message hook keyboard at the application layer, and hijacked the dispatch function of Kbdclass driven by keyboard filter driver or the keyboard interrupt in the kernel layer.

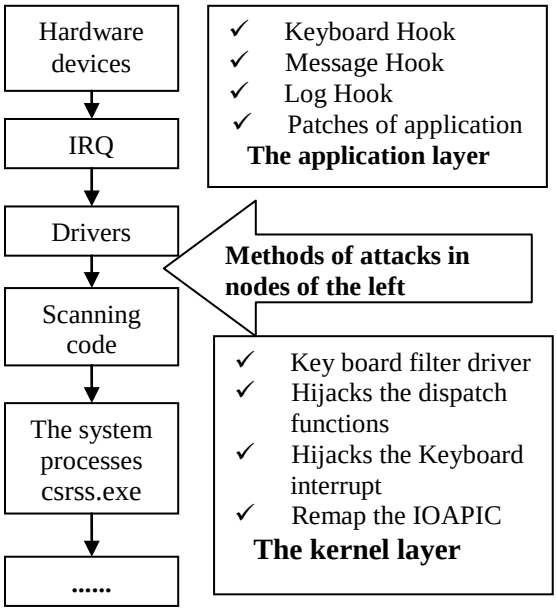

Figure 1: Relevant Nodes In The Process Of Logging Into The Online Banking

Part of the online banking chose the soft keyboard instead of inputting the user name and password directly, and it can partly increase the attacker's difficulty. However, sophisticated attackers can still obtain the actual information from the control of online banking or get the password through recording controlled client.

Figure 2 shows one solution of the attacks. It is to use the dispatch function of hijacked Kbdclass driven, pass the actual scanning code to the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ActiveX control directly. Then a randomly generated scanning code is used to replace the existent code in the keyboard driver, so that the attacker cannot get a real scan code from the keyboard filter driver. Nevertheless, a senior attacker can directly attack the ActiveX control that makes this method fail.

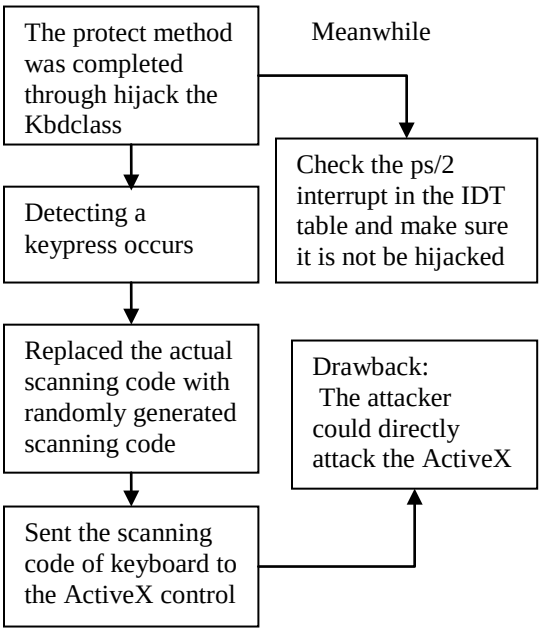

Figure 2: A Protective Measure That To Prevent The Attacker To Get The Use's Name And Password

The third type is tampering with the signature data.

Security is the primary concern of the online banking transactions. The lack of security may result in serious damages. Encryption may help make the transactions more secure that to protect the confidentiality of transaction data. Digital signature and authentication are also needed to guarantee that no one alters the data at either end of the transaction and to protect data's reliability and non-repudiation.

There are two forms of digital certificates, one is based on file and the other based on smart card. File digital certificate stored in the computer, system will call the private key in the file certificate when needs to sign. Because the certificate stored in the computer, the illicit operator can make a signature by reading the file digital certificate and resulting in illegal transactions. Client trading system based on smart cards is relatively safe. The private key is stored in the smart card, and the signature operation can only be performed within the hardware device.

Although the attacker could not use hardware devices for any data to be signed, aggression behavior could bypass the smart card, and they generally occurred when the user filled in the account number to be transfer and amount, and clicked the OK button, submitted a message to the server. The attacker put a program in the user's computer through planting Trojans, intrusion computer or email spoofing technology. When users opened the IE browser to access online banking address, the attacker got the accessing behavior and implants the intrusive programs in the user's IE browser. Attack tampered with the data which contains the transaction amount or the target account data to be trading by hijacking browser interface function such as HttpSendRequest, InternetReadFile and CSP, and then put the data into the smart card to sign.

Digital signature technology based on smart card had been very popular. Due to the signing process is implemented in hardware, and the private key cannot be exported from hardware, the security of the system based on smart card is relatively high, and many researchers work in this field. However, valid attacks generally bypass the smart card. At nowadays users are using the first generation of smart card, and the signing process is done automatically by the hardware. Users could not confirm the actual signature data put into the smart card.

4. ANALYSIS OF ATTACK PROCESS IN THE TRANSACTIONS

The attacker has two places to attack; one is tampering with the signature data, and the other is tampering with the user's transaction page to the transaction stage. The first point of attack is used to change the pending signature data and sent to the smart card to obtain the signature of forged data. The second point of attack used to deceive users, and enables the user to confirm that the submitted information (including user count and transaction amount) is true. At present, most online banking systems are simply better support IE browsers, so the attack programs need to be injected into the browser first. The way which specific DLL file into the IE browser is beyond the scope of this article, and it would not be discussed here. The following assumes that the user account CCount, target account to be transferred TCount, the amount TMoney, the attacker's account FCount, and the false transfer amount FMoney. The following is the analysis of user transactions attacked in details.

Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 1, the attacker planted Trojan on a user's computer in some way.

Step 2, the user opened the address of the IE browser to visit online banking. The Trojan monitored the IE browser had been launched and put the attack programs into the browser at the same time.

Step 3, the user (CCount) login to online banking, and filled in the transaction account (TCount), amount (TMoney) and clicked on the submit button on the page.

The scripts in the button extracted the information on the page and merged the data to be signed. The proposed transaction information could be simply described as

$$TSignMessage = CCount \,||\, TCount \,||\, TMoney \quad (1)$$

(Step 4) IE browser was ready to use the function of HttpSendRequest to send the information SignMessage to the server of the online banking.

Step 4, Attack procedures hijacked HttpSendRequest, modified TCount in TSignMessage to FCount, TMoney to FMoney. The signature information was modified to

$$FSignMessage = CCount \,||\, FCount \,||\, FMoney \quad (2)$$

, and submitted to the server by HttpSendRequest.

Step 5, the server returned the confirming information which was FSignMessage at this time.

(Step 6) IE browser would use InternetReadFile to receive confirmation on page.

Step 6, attack procedures hijacked InternetReadFile, search the keyword FCount and FMoney and replaced they with TCount and TMoney in the memory.

Step 7, the user received the confirmation page, and clicked on the OK button.

(Step 8) The scripts in the button called the hash [18] function CPHashData which provided by CSP to get a hash data (HTSM) from TSignMessage, and then called CPSignHash to get a signature (SHTSM) from HTSM.

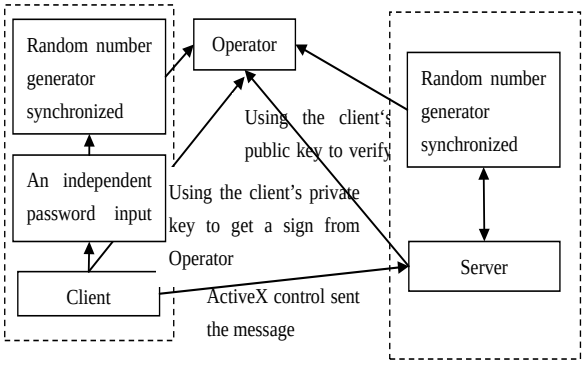

Figure 3: An Optimization Model Of The Online Banking

The hash and signature operation provided by CSP could either use the software or the smart card to complete; the specific manner did not affect aggressive behavior.

Step 8, the attack program hijacked CPHashData and replaced TSignMessage to FSignMessage and got corresponding hash value HFSM and signature data SHFSM.

Step 9, HttpSendRequest would send the signature be modified to the server.

As the plaintext matched the signature, it could be verified by the server; the money would be transferred to the tampered target account and returned the successful transaction page.

5. DESIGN OF SECURE PAYMENT SYSTEM

The highest security objective of online banking is to obtain the highest level of defending in a putative unsafe environment. Assuming that the computer was completely controlled, the user's trading can also be controlled within a range of security. Based on the above analysis of the means of attack and security of the online banking payment system, a design is given below (see figure 3).

In the design, it generated random numbers through synchronize the random number generator in the client and server. The transaction pin of user would input through the keyboard of the smart card and process with the random number (for example, used a self-designed hash function) before submited to the server for authentication. It could avoid the transaction pin delivered as a plain text in the data communication channel. Servers sent the confirming information to the client and also sent SMS as a means of multi-factor authentication.

First, because of the dynamic pin, the real user transaction pin did not appear in plain text in the client device. In the design of the smart card, there was a random number generator synchronized with the server. The random number would be generated in real time and joined the operation with user's transaction pin to generate transaction verification code. It would be encrypted with the use's private key never be out of the smart card and transferred to the online banking server to validate. This would ensure that the real transaction pin was not leaked. The server could use the user's public key in the public key certificate to verify.

Second, it used the second-generation smart card with a display device. Storing private key certificates with smart card could guarantee the safety of itself and the signature process.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The second-generation smart card with a display device, adding human intervention, could make the user to confirm before signing the specific data and to ensure it was not be modified to prevent the third type of attacks.

In addition, users should be prevented from inserting a smart card into the computer for a long time, only to insert it when need to use, which could enhance the security.

6. CONCLUSIONS

With the amount of users increased in online banking and trading, online banking system are becoming more desirable targets for attacks. This situation has prevented, in many cases, the development of online banking. The security problem has become the focus everybody cares.

Security issues in the online banking payment system include many aspects, such as business processing in the server, the user's private information leakage, using security and so on. This article focused on payment systems in the unsafe factors and attacks on the technical level, the means of three types of attacks and the security analysis were summarized. Based on the analysis in details and discussion with attack processes in the user transactions, security schemes were given that have the ability to fight against the attack means. The study would be useful for related researchers to improve their online payment schemes.

ACKNOWLEDGEMENTS

This work was supported by the cultivate fund of Xi'an University of Science and Technology No. 2010031 and No.201127.

REFRENCES:

[1] Claessens, J., V. Dem, D. De Cock, B. Preneel and J. Vandewalle, "On the security of today's online electronic banking systems", *Journal of Computers & Security*, Vol.21, No.3, 2002, pp. 253-269.

[2] Shi-Ming Huang, Wei-Cheng Shen, David C. Yen, Ling-Yi Chou, "IT governance:Objectives and assurances in internet banking", *Advances in Accounting*, Vol.27, 2011, pp.406-414.

[3] Cheolho Yoon, "Antecedents of customer satisfaction with online banking in China: The effects of experience".*Computers in Human Behavior*, Vol.26, 2010, pp.1296-1304.

[4] Saad M. Darwish, Ahmed M. Hassan, "A model to authenticate requests for online banking transaction". *Alexandria Engineering Journal*, In Press, Corrected Proof, Available online 11 April 2012.

[5] Granova, A. and J.H.P. Eloff, "Online banking and identity theft: Who carries the risk?", Computer *Fraud and Security*, Vol.11, 2004, pp.7-11.

[6] Stallings, W., "Cryptography and Network Security Principles and Practice, thirded", Prentice-Hall of India Pvt. Ltd., India, 2003.

[7] IEEE STD 1363-2000, "Standard Specifications for Public-key Cryptography", 2000.

[8] KOC CK, "High-speed RSA implementation", RSA Laboratories Technical Report, TR 801, V.1.0, 1996.

[9] Winn, J.K., "The Emperor's new clothes: The shocking truth about digital signatures and internet commerce", Idaho L. Rev, 2001.

[10] Housley, R., W. Polk, W. Ford and D. Solo, "Internet X.509 public key infrastructure certificate and Certificate Revocation List (CRL) profile", 2002, RFC 3280.

[11] Oded Goldreich, "Foundations of Cryptography, Volume 1: Basic Tools", Cambridge University Press, 2001.

[12] "Microsoft CryptoAPI and Cryptographic Service Providers", Available from: http://msdn.microsoft.com/en-us/library/bb931357(VS.85).aspx, 2012.

[13] ANSI X9.62-1999, "The elliptic curve digital signature algorithm (ECDSA)", Technical Report, American National Standard for Financial Services, Public Key Cryptography for the Financial Services Industry, USA, 1999.

[14] S. Basagiannis, P. Katsaros, A. Pombortsis, "Intrusion attack tactics for the model checking of e-commerce security guarantees", Proceedings of the 26th International Conference on Computer Safety, Reliability and Security (SAFECOMP),Computer Science 4680, Springer-Verlag, 2007, pp.238-251.

[15] Binod Vaidya, Jong Hyuk Park, Sang-Soo Yeo, Joel J.P.C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment". *Computer Communication*s, Vol.34, No.3, 2011, pp. 326-336.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[16] Chun-Ying Huang, Shang-Pin Ma, Kuan-Ta Chen, "Using one-time passwords to prevent password phishing attacks", *Journal of Network and Computer Applications*, Vol.34, No.4, 2011, pp.1292-1301.

[17] Ronggong. Song, "Advanced smart card based password authentication protocol", *Computer Standards & Interfaces*, Vol.32, 2010, pp.321-325.

[18] FIPS, "Secure hash standard", Federal Information Processing Standards PUB 180-2, 2002.