Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp306-309)

A Study for Vulnerability Analysis and Security Reinforcement Plan of Accredited Certification Service

JONGHYUN BAEK, WONCHEUL LEE, SEOKLAE LEE, JAEIL LEE
Korea Certification Authority Central
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul
KOREA

Abstract: Accredited Certification Service which was begun with enforcement of Digital Signature Act on July 1, 1999 for secure *electronic transaction* with allow the legal effect to *digital signature*, have supported a secure electronic transaction such as *internet banking* and *on-line stocks*.
But, because ordinary people can obtain hacking tool easily by fast development of informationalization, security of Accredited Certification Service is threatened by *hacking*. In this paper, Analyzes vulnerability and security reinforcement plan of Accredited Certification Service.

Key-Words: Accredited Certification Service, Electronic Transaction, Digital Signature, Internet Banking, On-line Stocks, Hacking

1 Introduction

According as the necessity of PKI (Public Key Infrastructure, PKI) introduction is suggested for secure electronic transaction in e-business environment, the Electronic Signature Act enforced in 1999 and established NPKI(National PKI) for secure Accredited Certification Service[1].
Electronic Signature Act promotes electronic transaction services by grant legal effect to digital signature which is based on Public Key Cryptography technique. And that is assumed by over 11 million people use certificate until end of September, 2005. But, Accredited Certification Service can be revealed to threat of hacking, according as ordinary people can obtain hacking tool easily by development of a hacking technology and spread of super-high speed internet. Especially, accident that hack another person's PC through keyboard hacking program that a rudiments hacker could save easily in the Internet last May and withdraw 50 million won occurred.
In this paper, I will analyze the vulnerability of Accredited Certification and suggest reinforcement plan of security and reliability in electronic transaction. In section 2, introduce vulnerable points that threaten security of Accredited Certification Service. In section 3, suggest plan for security reinforcement of Accredited Certification Service.

2 Analysis of Accredited Certification Service vulnerability

Accredited Certification Service which was begun at domestic from 1999 for secure electronic transaction base preparation have used by means to offer security and reliability in electronic transaction service, and widely dispersed more than 11 million people uses end of September, 2005. But, Accredited Certification Service needed examination for security according as certificate management software which is used in internet banking service revealed vulnerability and accident occurred that withdraws 50 million won in another person account through internet banking hacking last May. Hereupon, in this section, I wish to analyzes several vulnerability been bringing on present Accredited Certification Service.

2.1 Internet Banking Hacking

Last May, hacking accident about Internet banking that hacks another person's PC and withdraws 50 million won in account occurred for the first time in domestic.
Criminal installs keyboard hacking program that can hook keyboard input of another person PC on sufferer's PC through Internet board, and then he obtained private information of sufferer such as account password, security card number. Finally, criminal being re-key of sufferer's certificate using

sufferer's private information for withdraws 50 million won.

Relevant accident can hear some vulnerability for cause that was possible. First, use of hacking prevention program was unprepared on Internet banking site. Hacking prevention program should be placed automatically to user PC for protection of personal information such as password in Internet banking, but financial agency supported installation of hacking prevention program selectively because of user's convenience. Thereby, when hacking prevention program is not placed to user PC, personal information could be revealed to hacker easily.

Second, it is utilization vulnerability of security card used by main means for Internet banking security. Security card which is consist of the number of 30 four figures table is used like one-time password when use Internet banking. But, because security card was consisted of the number of 30 passwords table, the value as one-time password can be lower by high re-use rate of equal security card number. Also, security card user is employed so that transaction is suspended at input fault more than three times, but relevant function is not applied rightly at re-connection in the case of some bank. Finally, accredited certificate re-key was available to hacking information. When digital signature generation key(Private Key) was loss, damage or revealed, user must revoked own accredited certificate and certificate re-keyed to new one. For certificate re-key of accredited certificate, user must get a confirmation of face-to-face identification by visiting relevant bank directly. But, because this caused fair discomfort to user, some services were allowed accredited certificate re-key through on-line identification to solved this, and hacker abuses this for certificate re-keyed sufferer's certificate in own PC. That is, several functions that permit for user convenience were acted by vulnerability preferably.

2.2 Certificate Management Software Vulnerability

When connect internet banking at certificate management software of user PC, malignancy code can be installed from vulnerability of ActiveX controller [2]. Thereby malignancy program that attacker can activated in user PC as follows.

① Attacker hacks site to get abroad malignancy program in the advance, or installs malignancy program through internet board.

② Attacker sends user E-Mail to lead user to malignancy program distribution site and induces contact to specification web board site.

③ User connect to malignancy program distribution site that attacker has made in the advance.

④ This time, malignancy program is installed and activated automatically to user PC.

⑤ Attacker acquires control authorization for PC and steals user's data.

Of course, there is not cause of vulnerability of Accredited Certification Service itself but vulnerability of certificate management software, and hacking that use this is satisfied following beforehand condition.

First, Malignancy program should be installed in user's PC. Second, hacker must send the message that allure sufferer to E-Mail or web board for hacking. Third, user should connect to malignancy site that hacker makes in the advance.

Therefore, accident possibility of these hacking is low in Accredited Certificate Service that use hacking prevention program and financial agency homepage, but Private Key, certificate, Password can be revealed to hacker through similar several hacking methods. Now, because most of user is stored own private key to hard disk with accredited certificate, encrypted private key and certificate can be revealed to hacker. Even if private key stores to mobile storage such as USB token, Smartcard, Floppy disk, etc., it is not 100% secure, and difference of security level is existed according to kind of mobile storage.

2.3 Keyboard Hacking

Nowadays, Method for personal information acquisitions are Phishing and using keyboard hacking program method such as Key-logger [4], because Phishing problem's countermeasure is not Accredited Certification Service side but user side, keyboard hacking method will introduce in this session.

Keyboard hacking program does to reveal keyboard input character of another person PC as refer in Internet banking hacking example before.

When user uses the Internet, keyboard hacking is achieved into hardware level, kernel level, system level, application level and internet explorer level.

Keyboard hacking in hardware level are existed three types such as directly monitoring method of keyboard port in keyboard controller chip, using vulnerability of interrupter control method, interrupter hooking

method. In kernel level, keyboard driver hooking method and USB HID(Human Interface Devices) hooking method are existed. Hooking method for system level is messaging hooking method that is hook the CBT(Core Based Tree) or GET message which is call from system. Hooking method for Application class level is hooks the windows class which is call from application such as subordination class, super class, etc. Finally, method that use the explorer's vulnerability is reveal the private information using MSHML limitation, KEYPRESS limitation that use DHTML, CHANGE limitation, SUBMIT limitation when user input the private information in web browser input window of internet explorer. Vaccine and keyboard hacking prevention program are installed in user PC for protect private information, and in this case, hacking detection ability of security solution is to be key point for private information protective.

3 Security Reinforcement Plan

Because various hacking threat and vulnerabilities exist to Accredited Certification Service that is according to refer in section 2, must protect user from hacking threat through preventive measure preparation. I will explain method for security reinforcement plan of Accredited Certification Service such as security for private key storage medium, certificate re-key procedure reinforcement.

3.1 Security Reinforcement for Storage medium

Usually, almost Accredited Certification Service user uses hard-disk for save medium of accredited certificate and private key, and some user uses mobile storage such as floppy diskette, USB storage, etc.

Actually, Smartcard and USB token are seldom uses for security storage and management of private information, accredited certificate, private key, etc. But, it is becoming target of hackers because accredited certificate and private key storage location is unifying and opened for interoperability between Accredited CA in Korea NPKI(National PKI). Although, private key was stored with encryption form by password, but user's certificate and private key which is stored in hard-disk, floppy diskette, USB storage can be revealed easily because acquisition of password is possible from various hacking methods.

Therefore, to use Accredited Certification Service securing without user's private key revealed, Smartcard or USB token that is embed microprocessor chip for key pair generation, digital signature, certificate verification is needed. Because these are no possibility that private key is leaked to outside because all arithmetic are achieved in device inside, these can use Accredited Certification Service safely. In case of use smartcard or USB token which is embed microprocessor for save private key and certificate, there is need to solve the problem for device driver support. For this, standard specification such as PKCS#11 for interface between certificate management software and these devices is needed [3].

3.2 Security Reinforcement for Certificate Re-key Procedure

When private key was loss, damage or revealed, user must revoked own accredited certificate and certificate re-keyed to new one. For certificate re-key of accredited certificate, user must get a confirmation of face-to-face identification by visiting relevant bank directly. But, because this caused fair discomfort to user, some services were allowed accredited certificate re-key through on-line identification to solve this.

When Certificate re-key through on-line identification, there is need private information such as account number, account password, personal ID number and one-time password. But, these information can be revealed easily to hacker from keyboard hacking.

Especially, security card is used in Accredited Certification Service as one-time password that is required best security, but security card's value is fall because subscriber can only use about 30 passwords, each password is four figures. That is, whole safety can be weak in case of one number among security card is exposed because re-use rate of same number is high.

Therefore, it is need security plan that increases password number of security card within scope that is not injure user's convenience for secure electronic transaction service offer and minimizes amount of information that is revealed to hacker. One-time password security can be reinforced by increasing password number with concocting password more than two among the number of 30 password of security card.

New password can be generated by mixing two numbers of fixed position in each password that is selected two password(21st and 16th) among password of relevant security card.

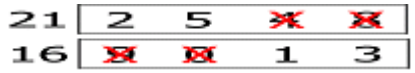

Fig 2 Example for Fixed Selection of Password

For example, new password(2513) can be generated by mixing top two digit of 21st password(2548) and back two digit of 16th password(9013). Because 870 passwords which were generated by mathematical equation 1 are available, re-use rate of equal password is low.

$$\text{Total Password Number} : N * (N-1) = 870 \quad (1)$$

N : Password Number of Security Card

Also, 31,320 passwords can be generated by password selection of random position without using password Selection of fixed position, but if consider overlap number, 10,000 password can be generated.
.

Fig 3 Example for Random Selection of Password

$$\text{Total Password Number} : (N * {}_4C_2) * ((N-1) * {}_4C_2) = 31{,}320 \quad (2)$$

N : Password Number of Security Card

3.3 Keyboard Hacking Prevention

Vaccine and keyboard hacking prevention program are installed in user PC for keyboard hacking prevention and these programs can be protected private information of user.
Therefore, hacking detection ability of security solution such as keyboard hacking prevention program is acted to key point. Keyboard hacking prevention program can prevent hardware level hooking and message hooking. But hooking for web browser input window can not prevented.
To prevent web browser input window hacking, it should be considered that general text input window must substitute with security input window for encrypt user private information.

4 Conclusion

Accredited Certification Service which was begun with enforcement of Digital Signature Act on July 1, 1999 for secure electronic transaction with allow the legal effect to digital signature, have supported a secure electronic transaction such as internet banking and on-line stocks. But, because ordinary people can obtain hacking tool easily by fast development of informationalization, security of Accredited Certification Service is threatened by hacking. In this paper, Analyzes vulnerability and security reinforcement plan of Accredited Certification Service. So that, it is important
Hereupon, recovery of Accredited Certification Service's trust through security reinforcement for storage medium and security reinforcement for certificate re-key procedure and Keyboard Hacking Prevention is to be important point. For the recovery of Accredited Certification Service's trust, the people and government should cooperates organically for solve the problem of Accredited Certification Service. Also, support the user guideline for secure electronic transaction utilization such as installation of Hacking prevention software and management scheme of password is need for the reinforcement of user security mind.

References:

[1] Youngchul choi, Kyounghee oh, Jaeil lee, Kiyung hong, Hongsup lee, *Establishment and Operation of Korea Certification Authority Central*, Journal of communication and Information Security, 1999
[2] Microsoft, *Browser Print Template and File Upload via Form Vulnerabilities*, Microsoft Security Bulletin MS00-093, 2002
[3] RSA Laboratories, *PKCS#11 : Cryptographic Token Interface Standard*, RSA Security, 2004
[4] Sachin Shetty, *Introduction to Spyware Keyloggers*, http://www.securityfocus.com/infocus/1829, 2005